Arcserve® Business Continuity Cloud

User Guide

arcserve

Legal Notice

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by Arcserve UDP at any time. This Documentation is proprietary information of Arcserve and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of Arcserve.

If you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all Arcserve copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to Arcserve that all copies and partial copies of the Documentation have been returned to Arcserve or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, ARCSERVE PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL ARCSERVE BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF ARCSERVE IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is Arcserve.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Contact Arcserve Support

The Arcserve Support team offers a rich set of resources for resolving your technical issues and provides easy access to important product information.

Contact Support

With Arcserve Support:

- You can get in direct touch with the same library of information that is shared internally by our Arcserve Support experts. This site provides you with access to our knowledge-base (KB) documents. From here you easily search for and find the product-related KB articles which contain field-tested solutions for many top issues and common problems.
- You can use our Live Chat link to instantly launch a real-time conversation between you and the Arcserve Support team. With Live Chat, you can get immediate answers to your concerns and questions, while still maintaining access to the product.
- You can participate in the Arcserve Global User Community to ask and answer questions, share tips and tricks, discuss best practices and participate in conversations with your peers.
- You can open a support ticket. By opening a support ticket online, you can expect a callback from one of our experts in the product area you are inquiring about.
- You can access other helpful resources appropriate for your Arcserve Support product.

Contents

Chapter 1: Documentation Overview

This section provides information about this guide and overall technical documentation available for Arcserve® Business Continuity Cloud. For example, getting started, key features, videos, links to other information not related to technical documents are listed under Related Documentation.

- **FAQs** helps with solutions of general questions and issues in respective guides.
- **Document Update History** helps you understand when a topic gets updated in this guide.

For further questions on documentation, click link to email us.

Important! In the document, the Console refers to Arcserve® Business Continuity Cloud Console.

This section contains the following topics:

About This Guide

Arcserve guide for customers helps you:

- Use the Arcserve® Business Continuity Cloud: Provides description of work flow and other role-based features.
- Understand function of every role: Provides separate sections for all roles that Arcserve® Business Continuity Cloud allows for an organization.
- Work with different additional features: For example, how to use Arcserve® Business Continuity Cloud Console.

Documentation of Related Arcserve Products

- Arcserve UDP Cloud Direct Bookshelf: r6.2.2
- Arcserve UDP Bookshelf: 7.0
- Arcserve Cloud Hybrid User Guide v1.1

Document Update History

Document Update History provides details about updates in this guide at different stages of Arcserve® Business Continuity Cloud Console.

Date of Update	Doc Version	Updates	Description
Oct 18, 2018	1.0	All topics new	Created new guide
May 31, 2019	1.1	Added one, updated multiple topics	**New Topic:** Set up UDP Cloud Direct Agent for Hyper-V **Modified:** Configure UDP Cloud Direct Virtual Appliance

Chapter 2: Understanding Arcserve® Business Continuity Cloud

Arcserve provides a single hosted, web-based management interface to help organizations centrally access, manage, and administer the Cloud Solutions. Arcserve® Business Continuity Cloud supports Arcserve UDP Cloud Direct completely and Arcserve Cloud Hybrid partially. The organizations interact with Arcserve either as direct customer or through MSP.

This section contains the following topics:

Overview

Arcserve® Business Continuity Cloud provides a unified, cloud-based management interface with access to robust technologies that allow businesses to backup and immediately restore access to critical data. Arcserve Cloud eliminates the need for multiple tools, vendors and management consoles.

User role and Access levels

User Roles and Access Levels

Arcserve® Business Continuity Cloud is accessible to two types of organizations. Direct customer organizations manage using two roles, while MSP-based organizations manage using three type of users. The access level of system varies for every user. Following users can perform tasks on the Console of Arcserve® Business Continuity Cloud:

Role Name	Created By	Key Functions	Comments
Direct Customer Admin (of Direct Customer)	Direct Customer enrollment for 1st Admin of Direct organization; Direct Admin creates more Admin on Console	• Monitors overall status of organization for backup and recovery jobs. • Protects sources, recovered sources, destinations and policies. • Analyzes jobs, logs and reports. Also, creates reports. • Configures infrastructure, source groups, access controls for users, licensing & subscriptions, and organization branding.	Role is applicable to direct organizations.
Direct Monitor	Direct Admin	• Applies filters • Views jobs, logs, and reports	Role is applicable to Direct organizations.
MSP Admin	MSP Customer enrollment for 1st MSP Admin; MSP Admin	• Monitors overall status of all customer accounts for job, licensed capacity, protected sources status, and destination usage trend. • Protects Customer account and adds customer account. • Analyzes jobs, logs and reports. Also, creates reports. • Configures access controls for users, licensing & subscriptions, and	MSP admin has access to everything for MSP and all customer's account. Role is applicable to MSP-based organizations.

		organization branding.	
MSP Account Admin	Assigned by MSP Admin	MSP Account Admin can administer and manage the assigned Customer Accounts with same functions as MSP Admin	MSP Account Admin is a user in MSP Organization. Manages customer accounts by MSP Admin. Role is applicable to MSP-based organizations.
Customer Administrator Admin (of Customer Account)	Created by MSP Admin	• Monitors overall status of organization for backup and recovery jobs. • Protects sources, recovered sources, destinations and policies. • Analyzes jobs, logs and reports. Also, creates reports. • Configures infrastructure, source groups, access controls for users, and organization branding.	End users administrator for MSP Customer Account Role is applicable to MSP-based organizations.
MSP Monitor	MSP Admin	• Applies filters • Views jobs, logs, and reports	Role is applicable to MSP-based organizations.

Two Factor Authentication (2FA)

Arcserve® Business Continuity Cloud supports two-factor authentication (2FA) that provides an additional layer of security to all the users. Two-factor authentication is a login process in which you are prompted to provide an additional form of identification. This method of authentication requires two factors for verifying your identity.

Two-factor authentication allows username and password as the first factor authentication. The second factor authentication uses the code generated through authenticator app.

Note: All the users have privileges to enable or disable two-factor authentication (2FA) from the User Profile page.

This section contains the following topics:

Enabling Two Factor Authentication (2FA)

You can enable two-factor authentication in the following ways:

- From the User Profile page
- Enabling requirement for 2FA at organization level
- From the Google Authenticator extension

This section contains the following topics:

How to Enable Two Factor Authentication (2FA) from the User Profile Page

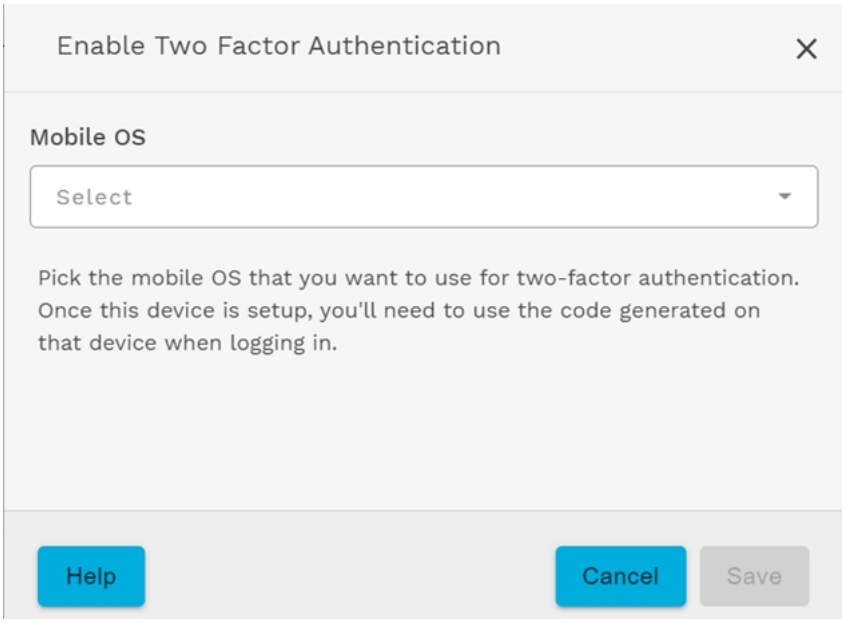
This section provides information about how to enable two-factor authentication from the User Profile page.

Follow these steps:

1. Log into the Cloud Console.
2. Click the user profile icon on the top-right corner, and then click **User Profile**.
3. Under the Two Factor Authentication section, enter the current password.

   The Enable Two Factor Authentication option gets enabled.
4. Click **Enable Two Factor Authentication**.

   The Enable Two Factor Authentication dialog appears.



5. On the Enable Two Factor Authentication dialog, from the Mobile OS drop-down list, select the mobile OS that you want to use for two factor authentication.

   The QR code image for logged-in user appears.
6. To scan the QR code image, download the Google Authenticator app on your mobile device, open the authenticator app, click the plus (**+**) symbol, and then click **Scan a QR code**.

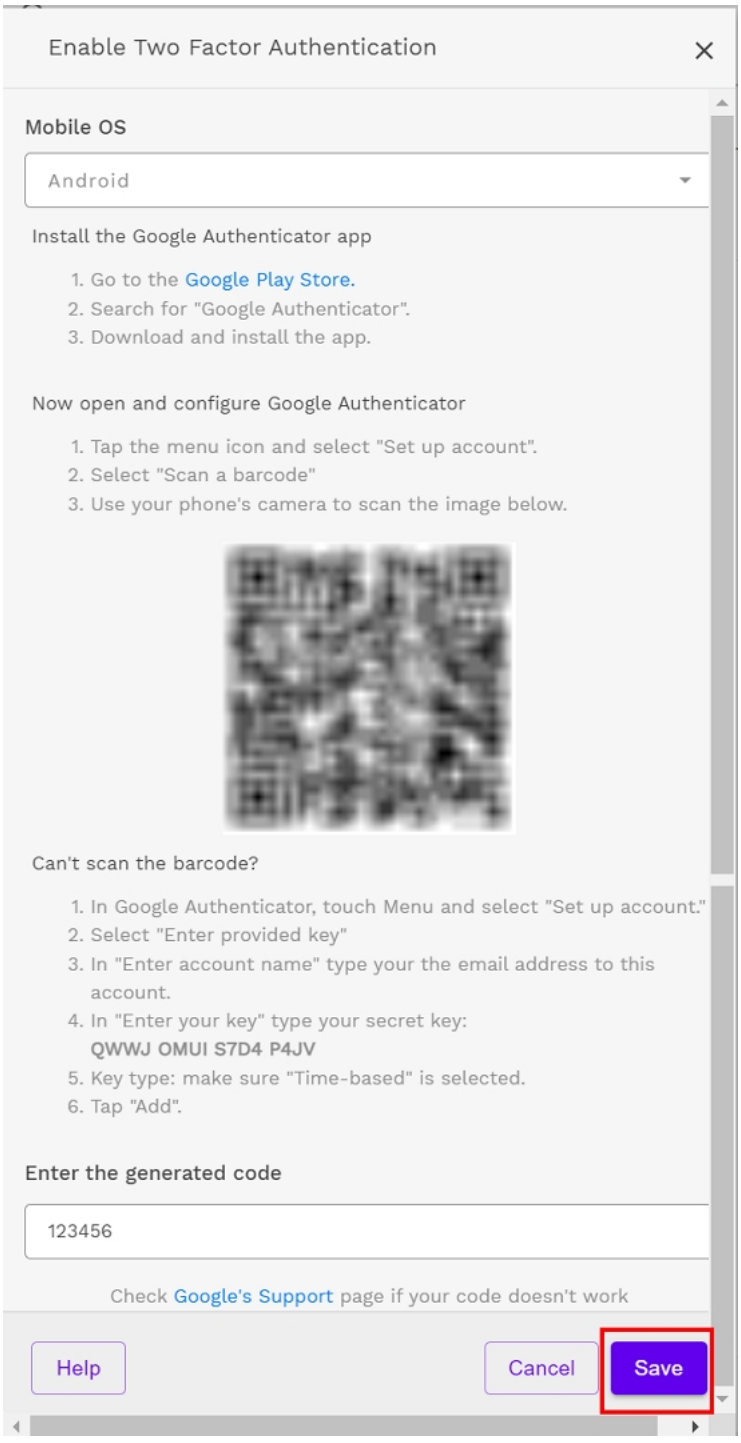
The corresponding cloud console account appears in the Google Authenticator app along with a 6-digit code.

Notes:

- Download the Google Authenticator app on your mobile device. Alternatively, you can also use the Authenticator extension on your Chrome browser.
- The code is valid for only 30 seconds and refreshes every 30 seconds.
- If you are unable to scan the QR code, do the following:
    a. On the authenticator app, click the plus (**+**) symbol, and then click **Enter a setup key**.
    b. On the Enter account details page, do the following:
        - **Account name:** Specify the email address linked with your account.
        - **Your key:** specify the secret key (example: 2P3Z 5BKI UX2L OTZQ). that appears on the Enable Two Factor Authentication dialog.
        - **Type of key:** From the drop-down list, select the Time based option.
    c. Click **Add**.

7. Enter the code generated, and then click **Save**.

   Note: If you click **Cancel**, the authentication fails.



The two-factor authentication (2FA) is enabled successfully.

Note: After 2FA is enabled, log out and login again. To log into the cloud console using two-factor authentication, see How to Log into the Cloud Console using Two-Factor Authentication.

How to Enable Two Factor Authentication (2FA) Requirement at Organization Level

When you require the use of two-factor authentication for the users who do not use 2FA, you can enable two-factor authentication requirement for all users at organization level. This section provides information about how to enable 2FA requirement at organization level.

Note: All the admin level users have privileges to enable two-factor authentication (2FA) requirement for all users.

Follow these steps:

1. Log into the cloud console.
2. Navigate to **Configure** > **Access Control** > **User Accounts**.
3. Click the **Two factor authentication required for all users** check box.

   Note: After selecting the *Two factor authentication required for all users* check box, if you navigate to the Monitor tab or logout and login again, you are prompted to enable two-factor authentication. To enable, follow the procedure from step 5 in the *How to Enable two-factor authentication from the User Profile Page* topic.

The two-factor authentication (2FA) requirement is enabled successfully.

Notes:

- When the tenants try to log into their respective accounts after the two-factor authentication (2FA) requirement is enabled at organization level, the 2FA authentication dialog pops up. To enable 2FA, configure the settings.
- When 2FA requirement is enabled at organization level and the tenants lost their 2FA code, only the Direct Customer, MSP Administrator, and MSP Account Administrator have privileges to reset 2FA code for their tenants.

Enabling 2FA Requirement through Impersonation View

The MSP Administrator and MSP Account Administrator have privileges to enable 2FA requirement for their tenants through impersonation view. This section provides information about enabling 2FA requirement through impersonation view.

Follow these steps:

1. Log into the cloud console.
2. Go to **Protect**.
3. To impersonate user, click the impersonate  icon next to the customer's name.

   The UI of the impersonated user appears.
4. Navigate to **Configure** > **Access Control** > **User Accounts**.
5. Click the **Two factor authentication required for all users** check box.

The 2FA requirement is successfully enabled for the tenants.

How to Enable Two Factor Authentication (2FA) using an Authenticator Extension in Google Chrome

Before enabling Enable Two Factor Authentication (2FA), add Authenticator extension in Google Chrome.

This section contains the following topics:

How to Add Authenticator Extension in Google Chrome

This section provides information about how to add Authenticator extension in Google Chrome.

Note: Make sure the Google Chrome is already installed before adding the Authenticator extension.

Follow these steps:

1. Open Google Chrome.
2. Search for Authenticator in the search bar.
3. Click **Add to Chrome** next to Authenticator.

   The message appears asking you to add extension.
4. Click **Add extension**.
5. The extension is added successfully. Chrome now displays the Authenticator extension icon on the top-right corner of your browser window, next to the address bar.
6. To give an extension access to the site, click the extension icon, and then click the pin symbol.

The Authenticator extension is successfully added in Google Chrome.

Enabling 2FA using an Authenticator Extension in Google Chrome

This section provides information about how to enable 2FA using an Authenticator extension in Google Chrome. If you do not want to use your mobile device for two-factor authentication, use the Authenticator extension in Goggle Chrome. Authenticator generates two-factor authentication (2FA) codes in your browser.

Follow these steps:

1. Open Google Chrome and then click the Authenticator app icon on the top-right corner of the address bar.

   The Authenticator dialog appears.

2. On the Authenticator dialog, click the **Scan QR Code** symbol on the top-right corner.

3. To scan the QR code, drag the **+** on QR code.

   The corresponding cloud console account gets created in the Authenticator dialog along with a 6-digit code.

4. Click the 6-digit code to copy.

   Notes:

   - The code is valid for only 30 seconds and refreshes every 30 seconds.
   - If you are unable to scan the QR code or do not want to scan the code, do the following:

     a. Click the Authenticator app icon on the top-right corner of the address bar.

     b. Click **Edit**  .

     c. Click **+** symbol, select **Manual Entry**, and then do the following:

        - **Issuer:** Type the account name of your choice.
        - **Secret:** Enter the 6-digit code generated in step 4.

     d. Click the **Advanced** drop-down, and then select the **Time Based** option from the Type drop-down list.

     e. Click **Ok**.

The two-factor authentication (2FA) is enabled successfully.

Disabling Two Factor Authentication (2FA)

You can disable two-factor authentication (2FA) in the following ways:

- From the User Profile page
- Disabling 2FA requirement at organization level

This section contains the following topics:

How to Disable Two Factor Authentication from the User Profile Page

This section provides information about how to disable two-factor authentication from the User Profile page.

Follow these steps:

1. Log into the Cloud Console.
2. Click the user profile icon on the top-right corner, and then click **User Profile**.
3. Under the Two Factor Authentication section, enter the current password.
4. Click **Disable Two Factor Authentication**.

The two-factor authentication (2FA) is disabled successfully.

How to Disable 2FA Requirement at Organization Level

You can disable two-factor authentication requirement for all users at organization level. This section provides information about how to disable two-factor authentication requirement at organization level.

Follow these steps:

1. Log into the cloud console.
2. Navigate to **Configure** > **Access Control** > **User Accounts**.
3. Unselect the **Two factor authentication required for all users** check box.

   A message appears asking you to configure additional settings to disable two-factor authentication (2FA) on the User Profile page.

   Notes:

   - After 2FA is disabled at organization level, all users must explicitly navigate to User profile page to disable 2FA.
   - To disable two-factor authentication for a particular user, do the following:

     a. Click the **Action** drop-down list next to that user, and then select **Reset Two Factor**.

        The confirmation message appears asking you to disable two-factor authentication.

     b. Click **Reset User Two Factor** to confirm.

   The two-factor authentication is disabled for that user successfully.

The two-factor authentication (2FA) requirement is disabled successfully.

Disabling 2FA Requirement through Impersonation View

The MSP Administrator and MSP Account Administrator have privileges to disable 2FA requirement for their tenants through impersonation view. This section provides information about disabling 2FA requirement through impersonation view.

Follow these steps:

1. Log into the cloud console.
2. Go to **Protect**.
3. To impersonate user, click the impersonate icon next to the customer's name.

   The UI of the impersonated user appears.
4. Navigate to **Configure** > **Access Control** > **User Accounts**.
5. Unselect the **Two factor authentication required for all users** check box.

The 2FA requirement is successfully disabled for the tenants.

Note: After the 2FA requirement is disabled for the tenants, the respective tenant users need to disable 2FA from the User Profile page.

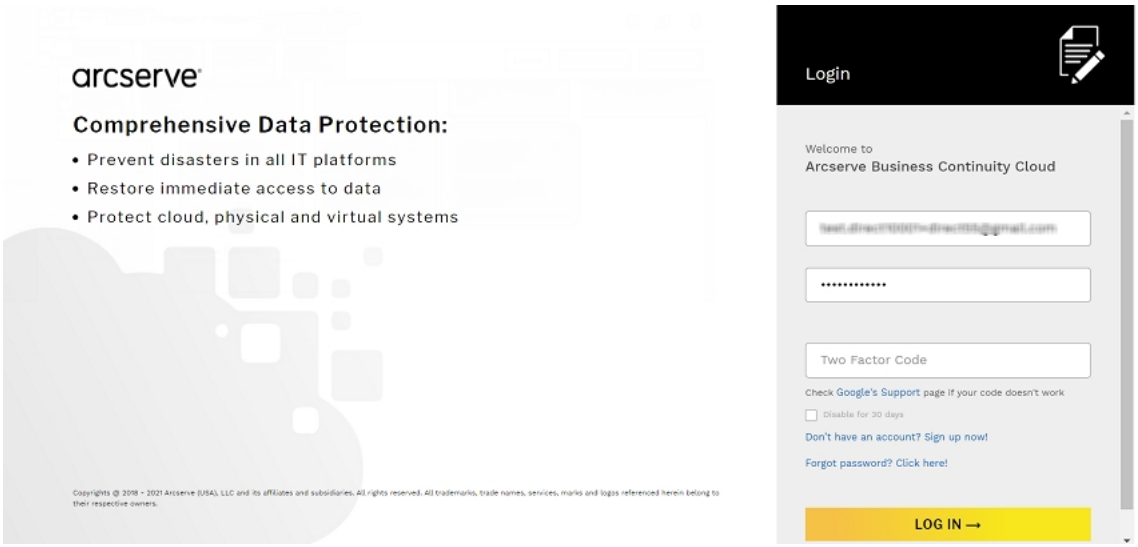
How to Log into the Cloud Console using Two-Factor Authentication

To log into the cloud console using two-factor authentication, you are prompted to enter the two-factor code along with the username and password.

This section provides information about how to log into the cloud console using two-factor authentication.

Follow these steps:

1. Go to the Arcserve® Business Continuity Cloud login page.



2. Type the username and password as needed.
3. In the *Two Factor Code* field, enter the two-factor code.
4. (Optional) To disable two-factor authentication for 30 days, click the **Disable for 30 days** check box.

   Note: If you select the *Disable for 30 days* check box and try to log into the console for the first time, you are prompted to enter the two-factor code. From the second time onwards, you are not asked to enter the two-factor code for 30 days unless you disable 2FA from the User Profile page.
5. Click the **LOG IN** button.

You are now successfully logged into the cloud console.

Notes:

- After enabling two-factor authentication, to generate two-factor codes for future use, do the following:

  a. Navigate to user profile icon on the top-right corner, and then click **User Profile**.

  b. Under Two Factor Authentication section, click **Generate Two Factor Codes**.

     The *one-Time Codes* dialog appears displaying 8 codes.

  c. Copy and save the codes in a safe location.

     Important! You cannot retrieve codes after closing the dialog. You need to generate codes again.

  Notes:

  - You can use each code only once.
  - Any previously generated codes are invalid.
  - You can generate codes multiple times.

- If the administrators have already enabled two-factor authentication and lost their mobile device along with the generated codes, contact Arcserve support.
- If the users have already enabled two-factor authentication and lost their mobile device along with the generated codes, contact MSP Administrator or MSP Account Administrator.

Chapter 3: Using Arcserve® Business Continuity Cloud as Direct Customer

Using Arcserve® Business Continuity Cloud, a direct customer can monitor jobs, protect sources and destinations, analyze jobs and reports, and configure the Console for own organization by adding users, customizing branding, creating source groups and configuring infrastructure.

This section contains the following topics:

Dashboard

After logging into Arcserve® Business Continuity Cloud, you land on the Console dashboard where you can view multiple common options and the details of Monitor feature. From the Dashboard, you can change password, update user details, view details to contact support, view important messages and log out.

Dashboard provides the following options:

- **Arcserve Icon:** Click on the Arcserve icon, placed on the top-left corner, and return to dashboard from anywhere in the Console.
- **Help Icon:** The Help icon on top-right takes you to the **Support** page where you can opt from multiple options to contact Arcserve and view Online help for the Console.
- **Alert Icon:** The exclamation mark icon on top-right displays messages from the Console for your consideration. The messages are categorized as **Critical**, **Warning** or **Information**. You can Acknowledge the messages and take action when required. For more details, view How to Manage Alerts.
- **User Login Icon:** The icon on top-right corner displays the profile picture of the logged-in user. The icon provides option to log out from Cloud Console and update user profile of the logged-in user.

Using User Profile, you can make two updates:

- **Update Contact Information:** From **My Profile** screen, you can update your contact details and upload photo. Click **Save Changes** after making updates.
- **Change Password:** Provide a new password and click **Update Password**.
- **Two-Factor Authentication:** Provide the current password, and then do one of the following:
  - To enable two-factor authentication, click **Enable Two Factor Authentication**.
  - To disable two-factor authentication, click **Disable Two Factor Authentication**.
  - To generate two-factor codes, click **Generate Two Factor Codes**.

Monitor

After logging into Arcserve® Business Continuity Cloud, you land on the Console dashboard where Monitor displays the details of your product using multiple wizards. From the Monitor, you can perform the following options:

- **View Summary:** Monitor displays Source Summary, Usage Summary and Policy Summary for the organization.
  - **Source Summary:** Displays the count of Total Sources and the count of sources with Protected, Offline or Unprotected status based on the last backup job result.
  - **Usage Summary:** Displays the usage summary of licensed capacity for Cloud Direct or Cloud Hybrid.
  - **Policy Summary:** Displays the count of Total Policies and the count of policies with Success, Deploying, Failure or Disabled status.

    Note: Clicking on the hyperlinked status terms leads you directly to the respective detailed screen. For example, from **Source Summary**, clicking **Protected** leads you to the Sources screen that displays the list of protected sources.
- **View Details as Graphs:** For better monitoring of key details, Monitor displays graphical view of multiple fields. For example:
  - **Backup Job Summary:** Displays the last 24 hours Backup Job count for Finished, Canceled, or Failed status. Hover over the graph to view the percentage for each status.
  - **Recent 10 Jobs in Progress:** Displays recent 10 jobs in progress, supports view log or cancel job action for all *in progress* job. Clicking **View all jobs** link leads you to the Jobs screen.
  - **Top 10 Sources:** Display top 10 sources per specific condition. Supports selected Backup Job Status, Events, Job Durations, and Data Transferred.
  - **Top 10 Polices:** Displays top 10 policies and group by Job status as Finished, Failed, Canceled, or Active.
  - **Usage Trend for Cloud Direct Volumes:** Displays Usage Trend for Cloud Direct Volumes by Full backup data and group by volume name.
  - **Usage Trend for Cloud Hybrid Stores:** Displays Usage Trend for Cloud Hybrid Stores and group by Cloud Hybrid Store name.

- **Data Transfer Summary For Cloud Direct Volumes:** Displays Data Transfer Summary for Cloud Direct Volumes and group according to Data Processed, Data Transferred, or Data Written.
- **Dedupe Savings Trends For Cloud Hybrid Stores:** Displays Dedupe Savings Trends For Cloud Hybrid Stores and group by Source Data or Dedupe Savings size.

- **View Cloud Hybrid Details:** View usage trend and dedupe savings trend for Cloud Hybrid Stores. Hover over the graph to view details.
- **Expand or Collapse widgets:** Use the icon placed above a displayed widget to expand or collapse.

Protect

Using the Console, you can protect Sources, Recovered Resources, Destinations, and Policies.

What's Next!

- Protect Sources
- Protect Recovered Resources
- Protect Destinations
- Protect Policies

Protecting Source

Using the Sources option, you can add sources or protect existing sources. A node refers to a physical or virtual source machine on hypervisors that you want to protect. You can protect a node by backing up data to a destination. From the Source screen, you can perform multiple options. For example:

- **Maximize of Minimize Source Screen:** Click the icon  placed on top to maximize the Source screen and to bring to default minimized size.
- **View Existing Sources:** The Source screen displays all the available sources with the details that you define in settings.
- **Define Settings:** Click the icon  to define options that you want to view for details of source. From the displayed list, select the options that you want displayed for sources.
- **Search Sources:** Provides multiple options to search added sources.
- **Save a Search:** Lets you provide a name to a search result and save with a unique name for future reference.
- **Manage Saved Search:** Lets you view all the saved searches and take collective action on any group. For more details, see How to manage saved search.
- **Actions:** From the Source screen you can perform either global or individual action on sources.

  For list of global and individual actions, view following links:

  - How to Perform Common Individual and Global Actions
  - How to perform individual actions for Cloud Hybrid
  - How to perform global actions for Cloud Hybrid
  - How to perform individual actions for Cloud Direct
  - How to perform global actions for Cloud Direct
- **Download Cloud Direct Agent:** Lets you download an agent that is required to add a source.
- **Add a Source:** Lets you add a new source. You must download an agent before adding a source.

View Existing Source

From the Source screen, you can view complete list of sources added before. With every source, multiple details are visible. Type, Source name and the action drop-down list at the end are default options.

For list of global and individual actions, view following links:

- How to Perform Common Individual and Global Actions
- How to perform individual actions for Cloud Hybrid
- How to perform global actions for Cloud Hybrid
- How to perform individual actions for Cloud Direct
- How to perform global actions for Cloud Direct

You can select other options to appear in the detail field according to your requirement. To customize, click the **Settings** icon  .

Some of the details displayed for source are as follows:

- **Type:** Refers to the type of source. The source is either a machine or a node on a Hypervisor.
- **Name:** Refers to the name of source. You can click the name and view details about a source. From the screen of source, you can perform multiple actions on a source. For more details, see Modify a Source.
- **OS:** Refers to the operating system of the source. The operating system is Windows, Linux or Mac.
- **Status:** Refers to the current status of the source. A source is either protected or not protected.
- **Connection:** Refers to the online or offline status of the source based on the connection to Internet.
- **Latest Recovery Point:** Displays the date and time of last recovery.
- **Latest Job:** Refers to the name of a job or number of jobs performed recently.
- **Policy:** Refers to the name of policy assigned to a source.
- **Source Group:** Refers to the name of group or else number of groups assigned to the source.
- **VM Name:** Refers to the name of VM for the source.
- **Agent:** Refers to the name of agent linked to source.

- **Organization:** Refers to the name of organization assigned to the source.
- **Hypervisor:** Refers to the name of Hypervisor for the source.
- **Drop-down Option for Action:** The drop-down option at the end of details for a source lets you perform multiple actions on one source. This option is applicable only to one source. View details and prerequisites for individual actions of Cloud Direct and Cloud Hybrid.

Search Source

You can search sources using multiple filters. To search, you can either enter the name directly and click the search icon or else click the drop-down arrow available in the Search box to select one or more filters and click **Search**.

Some of the available search filters for source are as follows:

- **Protection Status:** Refers to the current status of the source. A source is either protected or not protected.
- **Connection Status:** Refers to the online or offline status of the source based on the connection to Internet.
- **Job Status:** Refers to the job status of the source. The status is one of the following: In progress, Finished, Canceled, Failed, Warning, Skipped, Stopped.
- **OS:** Refers to the operating system of the **Type** of source. The operating system is Windows, Linux or Mac.
- **Source Groups:** Refers to the name of group that you can select.
- **Protection Policy:** Refers to the name of policy that you can select.

You can also save a search with results. For more details, view Save Search.

Save a Search

You have performed a search. After viewing results, you want to keep the results with search term for future reference. How can you do that?

Arcserve® Business Continuity Cloud reduces your multiple search efforts. From the Console, you can opt to save search results with a unique name. When you *perform a search*, the search results appear on the screen and the search term is displayed below the Search box at the **Search results for:** option. You can opt to either **Clear All** search terms or **Save Search**.

To save, click **Save Search**. A dialog for Save Search appears. Enter a unique name in the **Save Search Name** box and click **Save Search**. A message confirms successful action. The saved search name appears always in front of **Saved Searches**. You can click the name to view results even later without having to repeat the search.

You can later delete or update a saved search using Manage Saved Search.

Perform Global Actions on Sources

From the Source screen, you can perform multiple actions on one or multiple sources together. Simply, select the checkbox of one or more sources and click the drop-down option of Actions on top of the screen. Selected options display the number of sources that you have selected.

From the drop-down list, you can perform multiple global actions on selected sources. Some of the global actions are listed below.

- **Start Backup:** Click to start backup for all the selected sources.
- **Cancel Backup:** Click to cancel backup for all the selected sources.
- **Assign Policy:** Click to assign same policy to all the selected sources. From the dialog of **Assign Policy**, select a policy that you want to assign and click **Confirm**.
- **Remove Policy:** Click to remove policy together from all the selected sources.
- **Delete:** Click to remove the selected sources from Console.

For list of global and individual actions, view following links:

- How to Perform Common Individual and Global Actions
- How to perform individual actions for Cloud Hybrid
- How to perform global actions for Cloud Hybrid
- How to perform individual actions for Cloud Direct
- How to perform global actions for Cloud Direct

Apart from these collective actions, you can also perform individual actions on a specific source. For more details, see Perform Individual Actions on a Source.

Perform Individual Actions on a Source

From the Source screen, you can perform individual actions on a specific source. Simply, select the drop-down arrow placed at the end of the source and select desired option from the list of displayed actions.

From the drop-down list, you can perform multiple individual actions on a source. Some of the individual actions are listed below.

- **Start Backup:** Click to start backup of the source.
- **Cancel Backup:** Click to cancel scheduled backup for the source.
- **Start Recovery:** Click to start recovery of the source.
- **Assign Policy:** Click to assign a policy to the source. From the dialog of **Assign Policy**, select a policy that you want to assign and click **Confirm**.
- **Remove Policy:** Click to remove policy from the source.
- **Delete:** Click to remove the source from Console.
- **Cancel Replication(In):** Click to cancel scheduled Replication(In) for the source.
- **Deploy Policy:** Select a source and click **Deploy** from contextual actions menu to deploy policy configuration for the selected source.

  Note: The following actions do not appear for suspended organization:

  - Start Backup
  - Assign policy
  - Remove policy
  - Deploy policy
  - Cancel Replication(In)

For list of global and individual actions, view following links:

- How to Perform Common Individual and Global Actions
- How to perform individual actions for Cloud Hybrid
- How to perform global actions for Cloud Hybrid
- How to perform individual actions for Cloud Direct
- How to perform global actions for Cloud Direct

Apart from these individual actions, you can also perform global actions together on multiple sources. For more details, see Perform Global Actions on Sources.

Download Cloud Direct Agent

Important! For trial organization, the 'Download Cloud Direct Agent' button is available when trail is activated from the Monitor page or Entitlements page.

Use the option to add sources from Windows, Linux, and Mac Operating Systems. For the selected operation type, you can also select the system type between 64 bit and 32 bit. After downloading, you need to complete deployment of agent and configure for Arcserve® Business Continuity Cloud. For more information, click link.

Notes: You can also download the .OVA file used for virtual Appliance, at the Download Cloud Direct Agent window.

Add a Source

Before adding a source, you must download an agent.

Follow these steps:

1. From the Source screen, click **Add a Source**.

   The Add Sources screen appears displaying the downloaded agents.

2. Select a Hypervisor.

   List of VMs available for selected Hypervisor is displayed.

3. From the list of displayed VMs, select desired VMs.

4. Click **Add Selected VMs**.

   Based on selection, sources are added as Machines or Agentless VMs.

   Warning: As each VM gets backed up in sequence, few of our customers experienced backup delays when they tried to back up more than 15 VMs from a single host. Your backup performance depends mostly on data change rate, disk performance, and network bandwidth. If you encounter such issues, please use multiple hosts. This warning is pertinent to only agentless machines running on VMware Hypervisors.

You can also modify configuration of an existing source. For more details, see Modify Source.

Modify a Source

You can modify the details of an existing source from the screen of that source. To reach the screen, simply click the name of a source. The details about source is categorized into four tabs:

- **Information:** The tab provides general information and also lets you perform individual action on the source. The tab also lets you download the Agent when you click the hyperlinked name of Agent. You can also perform all the individual actions on the source using the **Actions** drop-down option. For more information, view Perform Individual actions on a source.
- **Jobs:** Provides list of jobs associated with the source. Jobs are categorized according to the following status: Jobs in Progress, Failed Jobs, Canceled Jobs, and Successful Jobs. Clicking the name of jobs takes you to the job page that displays information about the respective job. View Job description, such as Name of job, type of job, status of job, policy associated with source, destination of recovery point, duration, start and end time of job.
- **Log:** The Log tab provides complete list of logs for the source. From the **Log** tab, you can search specific logs without saving the search. You can also **Export** the log as .csv file. The log of a source provides the following information:
  - **Date:** Refers to the date when log was generated.
  - **Severity:** Refers to the information related to severity.
  - **Generated from:** Refers to the location from where the log was generated.
  - **Job Type:** Refers to the type of job performed.
  - **Message ID:** Refers to the unique ID generated for the message of log.
  - **Message:** Refers to the details provided about the specific log.
  - **Job Name:** Refers to the name of job. You can click the name of a job to view job details.
- **Recovery Points:** The Recovery Points tab displays all the recovery points linked with the source. You can search the recovery points without saving the search. The Recovery Points list displays the following information:
  - **Created on:** Refers to the date and exact time when the recovery point was created.
  - **Contents:** Refers to the location of Recovery point.

- **Policy:** Refers to the name of policy associated with the source.
- **Destination:** Refers to the destination of recovery point.
- **Drop-Down:** The drop-down arrows let you perform multiple action on a recovery point. For example, you can select to **Pin** or **Recover** a recovery point.

Protecting Recovered Resources

Using Recovered Resources feature, you can view the list of resources that you have recovered. The recovered resources are categorized according to type. For example, Recovered VMs. A key benefit of Arcserve® Business Continuity Cloud Disaster Recovery is providing customers the ability to run virtual instances of protected systems in the cloud in the event that a disaster impacts their on-premises environment. The process of powering on virtual instances of servers in the cloud and leveraging the cloud as a recovery site is often referred to a Failover.

Considerations to create Recovered Resources for a source

- If the source is a machine, assign the source a Cloud Direct Disaster Recovery as a Service Policy.
- If the source is an agentless VM, ensure that the hypervisor policy destination is a Disaster Recovery destination. As a result, all sources in the hypervisor policy are added as recovered resources.

About Failover

The Failover process involves all steps necessary to ensure that a customer can leverage the cloud as they would their on-premises environment to continue running their critical business operations. Important aspects of the Failover process include powering on virtual instances of protected systems in the cloud and enabling secure connectivity to the recovered environment.

What's next!

- Activating Arcserve Business Continuity Cloud
- Connecting to the Arcserve Business Continuity Cloud

Activating Systems in the Arcserve® Business Continuity Cloud

To activate a system in the Arcserve® Business Continuity Cloud, follow one of the methods:

- From Protect > Sources, select the source and click **Provision** from the **Actions** menu. The system starts with the latest recovery point.
- From Protect > Recovered VMs, select the recovered VM and click **Provision** from the **Actions** menu. The system starts with the latest recovery point.
- From Protect > Sources, click the source and select the option of **view details**. From the source page, click the **Recovery Points** option, select a recovery point and click **Provision** from the action drop-down option. The system starts with the latest recovery point.
- From Protect > Destinations, click the destination and select the option of **view details**. From the destination screen, click **Recovery Points** option, select a recovery point and click **Provision** from the action drop-down option. The system starts with the latest recovery point.

You have activated the system in Cloud successfully. Now, you can connect to the Arcserve® Business Continuity Cloud.

Connecting to the Cloud

You can use multiple options for securely connecting to Arcserve® Business Continuity Cloud in order to leverage the virtual instances of recovered servers.

This section contains the following topics:

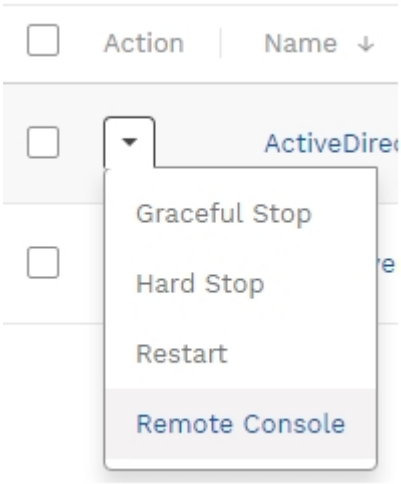
- How to Connect to Remote Console
- How to Connect to Point to Site VPN

How to Connect to Remote Console

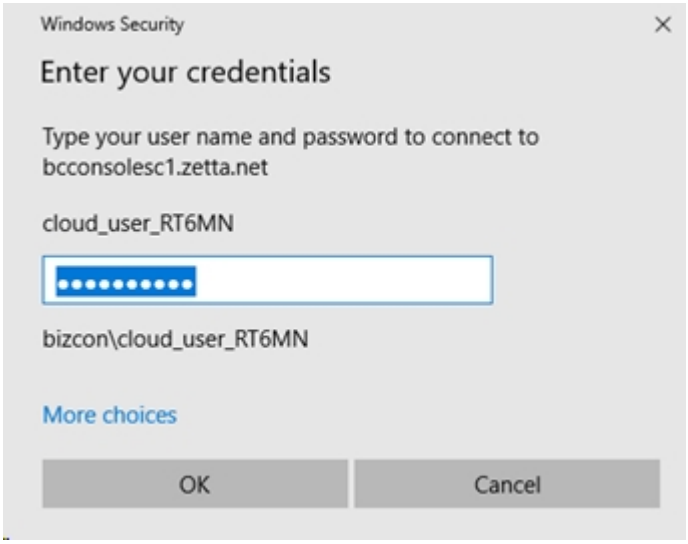
You can establish a remote console with a single virtual instance running in the Arcserve® Business Continuity Cloud. A remote console connection enables a user to access a virtual instance running in the cloud using the remote desktop protocol.

To establish a remote console connection with an activated virtual instance from the *Recovered Resources* page, follow these steps:

1. Click *Actions* > *Remote Console* for the activated system to download the remote desktop protocol (.rdp) file.



2. Launch the downloaded remote desktop protocol (.rdp) file.
3. Click *Connect* in the RemoteApp program dialog box.
4. Enter the password from the Login Credentials pop-up window into the Windows security dialog box.



5. Click *OK* to initiate the remote console connection. A web browser window should appear with the login screen of the virtual instance.
6. Click *Yes* when asked do you want to connect despite certificate errors.
7. Click Send Ctrl+Alt+Del at the top of the browser window.
8. Enter the Windows credentials for the virtual instance which are the same Windows credentials for the on-premises system at the time of the restore point.

You have connected to the remote Console successfully.

How to Connect to Point to Site VPN

A *Point to Site* connection enables a secure virtual private network (VPN) connection between a single client machine and the virtual private data center in Arcserve® Business Continuity Cloud. Such a connection would enable an end user at a coffee shop to establish a secure private connection to the recovered environment in the cloud.

Note: A separate connection is required if the end user also requires access to systems that are still available in the on-premises environment. The on-premises systems cannot communicate with the recovered systems in the cloud via the "Point to Site" connection.

To access the instructions that help to establish a *Point to Site* connection, navigate to Configure > Network Configuration, then click on **View Instructions**.

Protecting Destinations

A destination is a location where you store your backup data. A destination needs a recovery point server. Use the Destination tab to view and manage existing destinations. You can also add new destinations.

- Add a Destination
- View and Manage Destination
- Modify Destination

Add a Destination

Important! For trial organization, you can create destination after trial is activated from the Monitor page or Entitlements page.

To add a destination, you must have the data center that acts as server.

Note: You can add destination for Cloud Direct. To add destination for Arcserve UDP Cloud Hybrid, contact Arcserve Support.

Follow these steps:

1. From the Destination screen, click **Add Cloud Volume**.

   Add Cloud Volume dialog box appears with the **Account Name** displayed. Enter the following details:

   - Volume Name: Enter a unique name.
   - Data Center: Select from the available list of options.
   - Retention: Select the desired duration for retention.

2. Click **Add Cloud Volume**.

   The destination is added and you can view or modify from the Destination screen.

View and Manage Destinations

The Destination tab lets you view and manage destinations that are already added. From the Destination screen, you can perform the following actions:

- **Search Destination:** Use the search bar to provide filter option and search destination. You can also Save Search for future usage.
- **View Details about destination:** You can specify the details to view for a destination. Using Settings icon, select the options. For example, Storage Usage, Latest Job, Location, Data Center Region.
- Manage Destination: You can Edit or delete a destination. You can also View Recovery Points assigned to a destination.
  - **Edit** Destination: From the drop-down option of a destination, click **Edit** and modify the destination.
  - **View Recovery Points**: From the drop-down option of a destination, click **View Recovery Points**. From the Recovery points tab of that destination, you can view details about recovery points.
  - **Delete:** From the drop-down option of a destination, click **Delete**. A confirmation dialog appears. Click **Confirm** to delete.

    Note: You cannot delete if a destination is linked to a policy.

For list of global and individual actions, view following links:

- How to Perform Common Individual and Global Actions
- How to perform individual actions for Cloud Hybrid
- How to perform global actions for Cloud Hybrid
- How to perform individual actions for Cloud Direct
- How to perform global actions for Cloud Direct

You can also click the name of a Destination to modify and view Capacity Usage Trend.

Modify Destination

From Destination screen, click name of a destination to modify. The selected destination opens in new screen displaying the following three tabs:

- **Information:** The tab provides General information. You can update the **Name** and click **Save Changes**. You can also view following Information:
  - Cloud Direct: View information about Status, Region, Volume Type, Retention period.

    Note: Retention period is divided into hourlies, weeklies, monthlies, dailies, and yearlies. For more information, view how to use retention settings.
  - **Cloud Hybrid:** View information about Status, Region, Concurrent Active Nodes Limit, Source, Dedupe Savings, Policy, Storage Usage, and Latest Job. You can also view Deduplication and Compression status.
- **Recovery Points:** Lets you search the recovery points as well as recover or pin and also download the files/folder. From the tab, you can view following details about the selected destination:
  - **Created On:** Refers to the date and time of creation.
  - **Source:** Refers to the name of sources assigned.
  - **Contents:** Refers to the location of data.
- **Metrics:** Lets you view **Capacity Usage Trend** of the destination. You can select the number of days to view the report. The report provides information separated into Primary and Snapshot for Full Backup data.

Protecting Policies

A policy refers to the set of rule created to protect the data. Adding a policy requires a destination and configuring schedule to protect data.

Using the Policies feature in the Console, you can view the policies assigned to a source. From the screen, you can perform the following actions:

- **Search and Save:** You can search policies using multiple filters. To search, you can either enter policy name directly and click the search icon or else click the drop-down arrow available in the Search box to select one or more filters and click **Search**. You can also save a search with results. For more information, see Save Search.
- **View Policy Details:** From the policy screen, you can view list of available policies with the following details:
  - **Status:** Refers to the current status of policy such as Deploying, Disabled, Success, or Failure.
  - **Protected Sources:** Refers to the number of protected sources using the policy.
  - **Unprotected Sources:** Refers to the number of unprotected sources using the policy.
  - **Source Group:** Refers to the name or number of source groups using the policy.
  - **Latest Job:** Refers to the type of latest job. You can click the job type to view job details.
  - **Description:** Refers to the field displaying related details.
  - **Policy Type:** Refers to the field, which displays the type of policy created such as Cloud Direct BaaS, Cloud Direct DRaaS, Cloud Hybrid Replication, or Cloud Direct Agentless.
  - **Drop-Down:** Using the option, you can perform multiple actions on a policy. For example, delete or modify.
- **Modify a Policy:** To modify a policy, either use the **Modify** option available as individual action or click the name of a policy and on the policy screen to modify details of the policy. You can modify all the available policies of any protection type. You can also modify Hypervisor policy. For more information, view How to Modify a Hypervisor Policy.

- **Delete a Policy:** Select a policy and click **Delete** from the **Actions** menu to remove a policy.
- **Deploy Policy:** Select a source and click **Deploy** from contextual actions menu to deploy policy configuration for the selected source.
- **Add a Policy:** From the policy screen, you can create new policy. You cannot add policy for Hypervisor.

  To add a policy, view the following options:

  - Add a Policy for Cloud Direct Backup
  - Add a Policy for Cloud Direct Disaster Recovery
  - Add a Policy for Cloud Hybrid Replication
- **Enable Policy:** To enable a policy, from the **Policies** screen, using the **Action** drop-down list, click **Enable**. For more information, see Enable Policy.
- **Disable Policy:** To disable a policy, from the **Policies** screen, using the **Action** drop-down list, click **Disable**. For more information, see Disable Policy.
- **Global Action:** Select multiple policies and click **Actions** drop-down arrow from the top. From the displayed options, you can perform multiple actions on selected policies. For example, click **Delete** to remove all the policies.
- **Individual Action:** Click the drop-down arrow for a policy and from the displayed options, you can perform multiple actions on selected policy. For example, click **Delete** to remove a policy or click **Edit** to modify the details of existing policy.

  For list of global and individual actions, view following links:

  - How to Perform Common Individual and Global Actions
  - How to perform individual actions for Cloud Hybrid
  - How to perform global actions for Cloud Hybrid
  - How to perform individual actions for Cloud Direct
  - How to perform global actions for Cloud Direct

Add a Policy for Cloud Direct Backup

Important! The first policy is added by default on Enrollment for Direct Backup. Later, you can modify the policy or add new policies.

Notes:

- For trial organization, the default policy and destination are available when the trial is activated from the Monitor page or Entitlements page.
- If the organization gets suspended, **Add a Policy for Cloud Direct Backup** does not work.

Adding a policy for Cloud Direct Backup involves multiple steps.

Follow these steps:

1. From the Policy screen, click **Add Policy**.

   The Add policy screen appears with three tabs.

2. Click the first tab - **Basics** and perform the following steps:
   - Enter a **Policy Name**.
   - Select Cloud Direct Backup as the **Protection Type** .
   - Enter description if desired.
3. If you want to assign sources, click the second tab - **Source (Optional)** and perform the following steps:
   - You can use the **Search** box to find a matching source from the sources already added or else directly click **Select Source(s)** to view available sources.
   - From the displayed list of sources, select checkbox of one or more sources to add to the policy.

     Note: Add sources of the same operating system. For example, all Windows or Mac or Linux.
   - Click **Add Source(s)**.

   The screen displays added sources.
4. Click the third tab - **Destination** where you need to define the policy in detail.

   Provide the Activity Type, location to store, and schedule to protect. Perform the following steps in the three tabs:

Note: When the Activity Type selected is Cloud Direct file folder, the **Additional Settings** tab is also displayed. The Exclude configuration is available in the Additional Settings.

- From the tab, **What to protect**, select the desired activity for the policy.

  For **File Folder**, enter a UNC or local drive path for Windows or Linux path for (Mac/Linux). If a UNC path is entered, modify the run as user of the Cloud Direct Agent option to a user with full control on the UNC path and Builtin\Administrator permissions using either of the following options:

  - Start a backup and wait until the Cloud Direct Agent attempts to mount the UNC path. On the credentials prompt, the credentials that you enter is saved for future backups.
  - Right click the Cloud Direct Agent system tray icon and click **Local Settings**. Click **Browse** to find the desired user and then enter the password.

  For **Windows image**, you can opt either for Full System or specify one or more drives. A source configured with full system updates the list of drives that is backed up every time when the Cloud Direct Agent service starts.

  For **SQL Server**, select any one of the following:

  - **Sync direct from database:** Utilizes the SQL backup providers to stream the SQL database files and log files to the cloud without writing them to locally staged space.
  - **Sync via locally staged backup:** Verify if the staging directory is on a drive with free space greater than the total size of all the databases of all the instances that you are backing up. Verify if the selected user (with the option, run as user of the Cloud Direct Agent) has sysadmin privileges on the instances that you are backing up. By default the run as user of the Cloud Direct Agent is the NT Authority\SYSTEM user.

  For **Exchange**, you can backup the Microsoft Exchange Server database.

  Note: If multiple activity types are listed in What to Protect, you can configure each unique activity type by clicking the **Add Destination** button.

- From the tab, **Where to protect**, select a destination to protect the source. If you need to **Create a local backup**, enter a local path as the Destination that is not already getting backed up in the task configuration.

  Key Considerations:

  - If the sources in the policy are Windows System, then you can enter a UNC path or local drive path. If you select the Windows Image Backup>Full System task, use a UNC path to avoid performing a local backup to a drive backing up to the cloud as the Full System task backs up all drives.
  - If the sources are Linux or Mac systems, enter a Linux path.
  - If the tasks are non-File Folder tasks, then verify if you have 2.1 times the free space on the local copy destination as the Agent creates the new local copy first, then removes the old local copy. For File Folder tasks, the recommended free space is 1.1 times the size of the source path.
  - If a UNC path is entered, modify the run as user of the CD Agent to a user with full control on the UNC path and Built-in\Administrator permissions on the source system. To modify the run as user, right click on the Cloud Direct Agent system tray icon and click Local Settings. Then, click Browse to find the user and enter the password. Start a backup and wait until the Cloud Direct Agent attempts to mount the UNC path. On the credentials prompt, the credentials that you enter is saved for future backups.
  - Do not make a local copy to a sub-path of a path or drive that you are backing up to avoid duplicate data.

- The **When to protect** tab allows you to set a schedule for backup. Multiple backup schedules are available for BaaS policies such as Every 15 Minutes, Every 1 Hour, Every 6 Hours, and Every 1 Day with a Start Time. In addition, you can add a **Throttle Schedule**.

  Note: To enable multiple backup schedules for CD BaaS policies, contact **Arcserve Support**.

- From the **Additional Settings** tab, do the following:

  - For **Cache Location**, enter the location where the cache is stored. The Cache Location locally stores cache to optimize

transfer performance. It roughly totals 1% of the data set. If free disk space is a concern, provide an alternate location for the cache.

- For **Pre-backup Script**, enter the location of the script that executes before the backup job runs.
- (Optional) To stop the backup when script fails, check the **Stop backup if the script fails** checkbox.
- For **Post-backup Script**, enter the location of the script that executes after the backup is completed.

The Create Policy button is enabled.

Note: You can also remove a destination from the policy using **Remove Destination**.

5. Click **Create Policy**.

   The added policy is displayed on the Policies screen with the current status displayed as Deploying. After completion of deployment, the status changes either to Success or Failure.

Add a Policy for Cloud Direct Disaster Recovery

Prerequisites

- A license for Disaster Recovery.
- A DRaaS (zero copy) volume

Note: If the organization gets suspended, **Add a Policy for Cloud Direct Disaster Recovery** does not work.

Adding a policy for Arcserve® Business Continuity Cloud involves multiple steps.

Follow these steps:

1. From the Policy screen, click **Add Policy**.

   The Add policy screen appears with three tabs.

2. Click the first tab - **Basics** and perform the following steps:
   - Enter a **Policy Name**.
   - Select a Cloud Direct Disaster Recovery as the **Protection Type**.
   - Enter description if desired.
3. If you want to assign source, click the second tab - **Source (Optional)** and perform the following steps:
   - Click **Select Source(s)** to view available sources.
   - From the displayed list of sources, select checkbox of one or more sources to add to the policy.
   - Click **Add Source(s)**.

   The screen displays added sources.
4. Click the third tab - **Destination** where you need to define the policy in detail.

   Provide the Activity type, location to store, and schedule to protect. Perform the following steps in the three tabs:
   - From the tab, **What to protect**, select desired activity for the policy.

     For Windows image, you can opt either for Full System or individual drives. A source configured with full system updates the list of drives that are backed up every time when the Cloud Direct Agent service starts. If you select individual drives, make sure to include your boot drive.

- From the tab, **Where to protect**, select a disaster recovery destination to protect the source. If you need to **Create a local backup**, view the following considerations:
  - If you select the Windows Image Backup>Full System task, use a UNC path to avoid performing a local backup to a drive backing up to the cloud as the Full System task backs up all drives on each source in the policy.
  - If a UNC path is entered, modify the run as user of the Cloud Direct Agent option to a user with full control on the UNC path and Builtin\Administrator permissions on the source system. To modify the run as user, right click the Cloud Direct Agent system tray icon and click Local Settings. Click Browse to find the desired user and then enter the password. Another option is to start a backup and wait until the Cloud Direct Agent attempts to mount the UNC path. On the credentials prompt, the credentials that you enter is saved for future backups.
  - Verify if you have 2.1 times the free space on the local copy destination as the Agent creates the new local copy first, then removes the old local copy.
- From the tab, **When to protect**, set a schedule for backup. Multiple backup schedules are available for disaster recovery. For example, Every 15 Minutes, Every 1 Hour, Every 6 Hours, Every 1 Day with a Start Time. You can also opt to add a **Throttle Schedule**.

Create Policy button is enabled.

5. Click **Create Policy**.

   The added policy is displayed on the Policies screen with the current status displayed as Deploying. After completion of deployment, the status changes either to Success or Failure.

   After a successful deployment, a Recovered Resource is created for the source and visible at the Recovered Resources tab.

Add a Policy for Cloud Hybrid Replication

Note: If the organization gets suspended, **Add a Policy for Cloud Hybrid Replication** does not work.

Adding a policy for Arcserve® Business Continuity Cloud involves multiple steps.

Follow these steps:

1. From the Policy screen, click **Add Policy**.

   The Add policy screen appears with three tabs.

2. Click the first tab - **Basics** and perform the following steps:

   - Enter a **Policy Name**.
   - Select Cloud Hybrid Replication as the **Protection Type**.
   - Enter description if desired.

   The Source tab is disabled.

3. Click the third tab - **Destination** where you need to define the policy in detail.

   Provide the Activity type, location to store, and schedule to protect. Perform the following steps in the three tabs:

   - In the tab, **What to protect**, select desired activity for the policy.

     Replicate from a remotely-managed RPS. To configure this activity refer to **Replicate from a remotely-managed RPS** task in *Arcserve UDP Solutions Guide*.

   - In the tab, **Where to protect**, select a destination to protect the source.
   - In the tab, **When to protect**, set a Merge schedule.
   - In the tab, **Additional Settings**, you can also opt to add Retention Policy to retain **Daily Backups**, **Monthly Backups**, **Weekly Backups**, and **Manual Backup**.

   Note: You can also remove a destination from the policy using **Remove Destination**. But if you configured with the Replicate to a remotely-managed RPS task, you need to remove that first before removing the Replicate from a remotely-managed RPS task.

4. (Optional) From the third tab - **Destination**, add a new task **Replicate to a remotely-managed RPS** for reverse replication. To configure this activity

refer to **Replicate to a remotely-managed RPS** task in *Arcserve UDP Solutions Guide*.

- Click the cross icon to close the Replicate from a remotely-managed RPS task.
- Click the Hyperlink icon to add a Replicate to a remotely-managed RPS task.
- Click the Replicate to a remotely-managed RPS task.
- In the **Where to protect** tab, provide remote UDP Console access information to get share plan.
- In the **When to protect** tab, add Replicate Schedule and Throttle Schedule.

Note: You can also remove a destination from the policy using **Remove Destination**.

The Create Policy button is enabled.

5. Click **Create Policy**.

   The added policy is displayed on the Policies screen with the current status displayed as Success, Fail or Deploying. You can also modify the policy later. Click the policy name from the Policy screen and make updates.

   Note: You can protect Agent-based, OneDrive, CIFS, Agentless nodes of Arcserve UDP in Arcserve Cloud by configuring Cloud Hybrid Replication task. For more information, refer to Configure Replicate to Arcserve Cloud task.

Modify a Hypervisor Policy

You can modify policies for all protection types. Here is an example of how to modify policy of hyperfvisor.

Follow these steps:

1. From the Policy screen, click **Add Policy**.

   The Add policy screen appears with three tabs.

2. Click the first tab - **Basics** and perform the following steps:

   - Enter a **Policy Name**.
   - Select a **Protection Type**. For example, Cloud Direct Backup or Cloud Hybrid Replication.
   - Enter description if desired.

3. If you want to assign source, click the second tab - **Source (Optional)** and perform the following steps:

   - You can use the **Search** box or else directly click **Select Source(s)** to view available sources.
   - From the displayed list of sources, select checkbox of one or more sources to add to the policy.
   - Click **Add Source(s)**.

   The screen displays added sources.

4. Click the third tab - **Destination** where you need to define the policy in detail.

   Provide the source, location, and schedule to protect. Perform the following steps in the three tabs:

   - In the tab, **What to protect**, select desired activity for the policy.

     For Windows image, you can opt either for Full System or specify one or more drives

   - In the tab, **Where to protect**, select a destination to protect the source. If you need to **Create a local backup**, enter a local path as the Destination.
   - In the tab, **When to protect**, set a schedule for backup. You can also opt to add a **Throttle Schedule**.

   Create Policy button is enabled.

5. Click **Create Policy**.

   The added policy is displayed on the Policies screen with the current status displayed as Deploying. After completion of deployment, the status changes either to Success or Failure.

Analyze

The Analyze feature lets you view Jobs, Log, and Reports. The icon on top lets you collapse or expand the screen.

What's Next!

- Analyze Jobs
- Analyze Logs
- Analyze Reports

Analyzing Jobs

Displays complete list of jobs with the details that you can customize.

Key Highlights

- The search bar helps you find a job according to the selected filters. For example, status, job type, date range or protection policy.
- You can save the search also for future usage.
- Manage Saved Search option lets you manage a search if you have saved. For more information, view how to manage saved search.
- All the jobs display details that you can customize by using the Settings icon. Jobs are divided into multiple categories based on status. For example, Jobs in Progress, Failed Jobs, Canceled Jobs, and Successful Jobs.
- View Job description, such as Name of job, type of job, status of job, policy associated with source, destination of recovery point, duration, start and end time of job. You can also view the job description from the Jobs tab on the screen of a source.
- For every job, you can **view log**. Click the drop-down option placed at the end of every row of a job to view log of that job.
- You can also **Cancel** a job that is in progress.

  For list of global and individual actions, view following links:

  - How to Perform Common Individual and Global Actions
  - How to perform individual actions for Cloud Hybrid
  - How to perform global actions for Cloud Hybrid
  - How to perform individual actions for Cloud Direct
  - How to perform global actions for Cloud Direct

Analyzing Logs

The log tab displays all activity logs for the protected nodes, destination servers, data stores, and policies. You can view logs and apply various filters such as severity, logs generated from the machine, job type, and log content. You can also Export logs. Message ID provides a hyperlink to access detailed documentation. Click the hyperlink in the MessageID column to view the description and solution for that message. On the log screen, Message IDs are displayed only for Replication IN jobs.

Export Logs: From the Log screen, you can export the logs to your Inbox. Click **Export** from the top of Log screen and the log is sent to your registered email ID. In your inbox, find the email from Arcserve Cloud Support email with the subject Log Export and click **Download Export** in the email to download log as .csv file.

Search Logs: You can search the activity logs using a combination of the available filters or one of the following options and clicking **Search**:

- Select **Severity** types to view all the logs related to the selected type.
- Select **Job Type**.
- Select **Date Range**.
- Select **Generated From** location.
- Enter message term in the Search box.

Analyzing Alert Reports

Use Arcserve® Business Continuity Cloud to analyze alerts separately or together based on the alert type.

From the list of alerts, you can view alert details such as Alert Name, Alert Type, Report for, Created on, Last Generated, and Recipients.

From the Alerts screen, you can perform following actions:

- Create a New Alert Report
- Edit an Alert Report

Create a New Alert Report

Using **Create Alert**, you can add new alert report. The alert report is sent as a link to the email and additional recipients, if added. The **Create Alert** report wizard is required to create new report. The wizard appears when you click **Create Alert** on the alerts page.

Follow these Steps:

1. From the Analyze screen, click **Alerts** tab.

   The Alerts screen appears.

2. From the Alerts screen, click **Create Alert**.

   The Create Alert wizard appears.

3. From the **Create Alert** wizard, from **Alert Type**, select one of the options.
4. For Alert Name, enter a unique name for your new alert report.
5. Select one of the following options:
   - **Report all Sources:** Lets you generate report from all available sources.
   - **Report selected Source Groups:** Lets you generate report only from the selected source groups. If you select this option, from the drop-down option, select Source Groups, and then click **Add**. To select multiple groups, repeat the action.
6. (Optional) To share your report with others, enter email addresses of one or more recipients, and then click **Add**.
7. Click **Create**.

   A confirmation dialog appears that displays the successful generation of the alert report.

The Alert Report screen contains the success report. When the backup is completed, an email is sent to the logged in user and other recipients, if any.

Edit an Alert Report

You can edit an Alert Report in the Alerts page.

Follow these steps:

1. From the Analyze screen, click **Alerts**.

   The Alerts – Reports screen displays a List of reports. From the list, click the name of an Alert Report or use the drop-down option to select the report, and then click **Edit**.

   The Edit Report Settings screen appears.

2. From the screen, select one of the options to specify the sources:
   - **Report all Sources:** Lets you edit reports from all available sources.
   - **Report selected Source Groups:** Lets you edit reports only from the selected source groups. If you select this option, from the drop-down option, select Source Groups, and then click Add. To select multiple groups, repeat the action.
3. To share your report with others, enter email addresses of one or more recipients, and then click **Add**.
4. Click **Save Changes**.

   The report is modified.

Analyzing Reports

Arcserve® Business Continuity Cloud helps you analyze the report together as well as separately according to the report types. From the Report screen, you can search for reports using the filters of Date Range, Schedule for, and Generate on. Also, you can save the search item.

From the list of reports, you can view details about a report. For example, Report Name, Date Range, Report for, Generated on, Scheduled for, Report type, Created by, and Recipients. From the report screen and related screens, you can also perform following actions:

- Create Report
- View Reports
- Manage Report Schedules
- Export report
- Edit a report schedule

How to View a Report

Using the Console, you can view reports directly from the Report screen or navigate to a specific type to view related reports. From the report screen, you can perform the following actions:

- **View Details of Report:** The list of report displays all the reports including Backup Jobs reports, Recovery Jobs reports, Data Transfer reports, and Capacity Usage reports. You can use Search bar to filter the type of reports to view. Clicking the report name lets you view complete details in dashboard. You can delete one or multiple reports from the report screen.
  - **Delete A Report:** From the drop-down option placed at the end of a report, when you click **Delete Report**, a confirmation dialog appears. Click **Confirm** to delete the report.
  - **Delete Multiple Reports:** To remove multiple reports together, select check boxes of desired reports and select **Delete** from the drop-down option of **Actions**.
- **View Reports of Specific Type:** To view specific reports of only one type, navigate to any of the available report types. From report screen of specific types, you can also create a new report and export the report.

Available Report types:

- Backup Jobs
- Policy Tasks
- Recovery Jobs
- Data Transfer
- Capacity usage

Report for Backup Jobs

From the console, click Backup Jobs below Reports to reach the screen that lets you view summary of all the backup jobs. You can also search the source using the filters of Date Range, Protection Policy, Destination or Source Groups. Using multiple filters is allowed. Click icon of Manage Saved Searches to select the option that you want to view in report.

Key Highlights:

- From the screen, you can Create Report and Export Report as .csv file.
- Hover over the chart to view percentage of Failed, Finished, and Canceled jobs.
- View top 10 sources and filter according to Backup Job Status, Events, Jobs Duration or Data Transferred.
- Hover over the graph to view classification of Finished, Failed and Canceled jobs.
- View **Details** of all backup jobs from the table.

Report for Policy Tasks

To view the policy tasks details of completed backup jobs, go to **Analyze** > **Policy Tasks**.

Click **Policy Tasks** to view the summary of the policy tasks of completed backup jobs. You can search the source using multiple filters such as Date Range, Protection Policy, Destination, and Sources Groups. On the top-right corner of the **Policy Tasks** page, click **Manage Saved Searches** and select an option that you want to view in the report.

Key Highlights

- From the screen, to create and export report as a .csv file, click **Create Report** and **Export Report** respectively.
- Hover over the chart to view the percentage of Finished, Failed, and Canceled jobs.
- Apply filters to view Top 10 Sources such as Events and Job Duration.
- Hover over the graph to view classification of Finished, Failed, and Canceled jobs.
- From the table, view Details of all policy tasks for completed backup jobs.

Report for Recovery Job

From the Console, click Recovery Jobs below Reports to reach the screen that lets you view summary of all the jobs recovered. You can also search the source using the filters of Date Range, Destination or Source Groups. Click icon of Settings to select the option that you want to view in report.

Key Highlights:

- Hover over the chart to view percentage of Failed, Canceled, and Finished jobs.
- View top 10 sources and filter according to Recovery Job Status, Events, Jobs Duration or Data Transferred.
- Hover over the graph to view classification of Finished, Failed, and Canceled jobs.
- View **Details** of all restore jobs from the table.
- Export the reports as CSV file.
- Create reports for individual reports for all roles.
- Manage saved search. For more information, view how to manage saved search.

Report for Data Transfer

From the console, click Data Transfer below Reports to reach the screen that lets you view summary of data transfer. You can also search the source using the filters of Date Range and Source Groups.

Key Highlights:

- Hover over the chart to view data processed, data transferred and data written on a specific date.
- Hover over the graph to view classification of Finished, Failed and Canceled jobs.
- View **Details** of all data transfer from the table.
- Export the reports as CSV file.
- Create reports for individual reports for all roles.
- Manage saved search. For more information, view how to manage saved search.

Report for Capacity Usage

From the console, click Capacity Usage below Reports to reach the screen that lets you view usage trends and dedupe savings trend. You can also search the destination using the filters of Date Range, and Destination.

Key Highlights:

- Hover over the chart to view usage trend and dedupe saving trend on different dates.
- View **Details** of capacity usage from the table.
- View details about all available destinations.
- Export the reports as CSV file.
- Create reports for individual reports for all roles.
- Manage saved search. For more information, view how to manage saved search.

Manage Report Schedules

You can manage schedules of all the report using Manage Report Schedules. Under Analyze>Reports, click Manage Report Schedules and you can view list of all reports. From the screen, you can perform the following actions:

- **Search:** To search reports, either provide a report name in the search bar or use filters of **Scheduled for** and **Report Type**.
- **View details:** The list of report provides complete details about every report. For example, Report Name, Report Type, Report for, Scheduled For, Created by, Created on, Last Generated. You can click a Report Name to edit settings of the report.
- **Global Actions:** When you select check box of one or more report names, in the top bar **Selected** shows the number of check boxes selected and **Actions** option is enabled to help you perform collective action on selected reports. For example, **Delete** all selected reports or use **Generate Now** to prepare a copy of all selected reports.
- **Individual Actions:** On a specific report, you can perform the following individual actions:
  - **Edit Report:** From the drop-down option placed at the end of a report, when you click **Edit**, the dialog **for Edit Report Settings** appears. Make required modifications and click **Save Changes**. For more details, view how to edit a report schedule.
  - **Generate Now:** From the drop-down option placed at the end of a report, when you click **Generate Now**, an instance of that report is created and appears immediately in the list of reports.
  - **Delete A Report:** From the drop-down option placed at the end of a report, when you click **Delete Report**, a confirmation dialog appears. Click **Confirm** to delete the report.

    Note: While deleting report as individual or global action, you can also delete all report instances created by a report schedule. From the confirmation message, select the check box of **delete the report instances** also.

Configure

Arcserve® Business Continuity Cloud helps you configure multiple options to have better control. For example, you can configure infrastructure, source groups, access control, entitlements, and branding for organization.

What's Next!

- Configuring Infrastructure
- Configuring Source Groups
- Configuring Access Control
- Configuring Entitlements
- Configuring Branding

Configuring Infrastructure

Using Infrastructure feature, you can add Hypervisors to Arcserve® Business Continuity Cloud. The screen displays list of Hypervisors added for your organization. To add a hypervisor, you need to perform the following steps:

1. Set up UDP Cloud Direct Virtual Appliance
2. Configure UDP Cloud Direct Virtual Appliance
3. Delete UDP Cloud Direct Virtual Appliance

How to Set up UDP Cloud Direct Virtual Appliance

For VMware virtual environments, deploy the UDP Cloud Direct Virtual Appliance to enable agentless protection of one or more VMware virtual machines. The virtual appliance eliminates the need to install the UDP Cloud Direct agent on each virtual machine.

This section contains the following topics:

- Downloading UDP Cloud Direct Virtual Appliance
- Deploying UDP Cloud Direct Virtual Appliance
- Registering UDP Cloud Direct Virtual Appliance

Downloading UDP Cloud Direct Virtual Appliance

The UDP Cloud Direct Virtual Appliance is available as *.ova* file at the Arcserve® Business Continuity Cloud Console. From the Console, click **Download Appliance for VMware (.OVA)** from Configure > Infrastructure > Hypervisors to download the file.

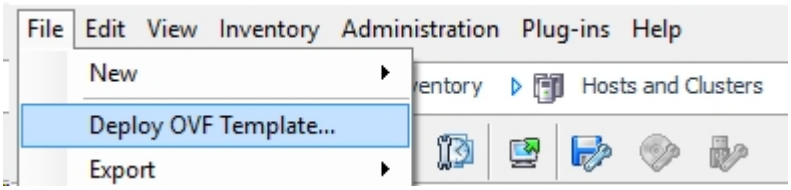
Now, you need to deploy the appliance.

Deploying UDP Cloud Direct Virtual Appliance

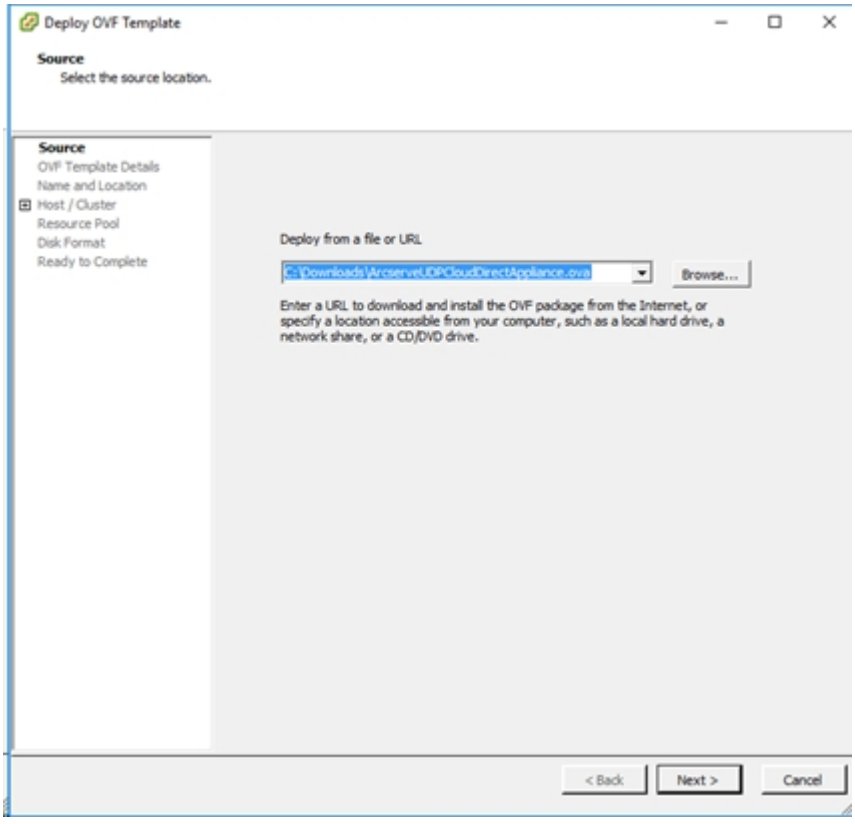
Use the VMware vSphere Web Client to deploy the UDP Cloud Direct Virtual Appliance into your VMware vSphere environment.

Follow these steps:

1. Launch the VMware vSphere Web Client and log in.
2. In the vSphere Web Client, click on File, and then select Deploy OVF Template.



3. Click ***Browse*** to select the file from the location where you downloaded the *.ova* file and click **Next >**.



4. Proceed through the rest of the setup process until you reach *Ready to Complete*, and then click **Finish**.

   The UDP Cloud Direct Virtual Appliance is deployed.

5. Once completed, click **Close**.
6. Navigate to *Getting Started* and select the UDP Cloud Direct Virtual Appliance, and then click *Power on the virtual machine*.

You have deployed the UDP Cloud Direct Virtual Appliance successfully.

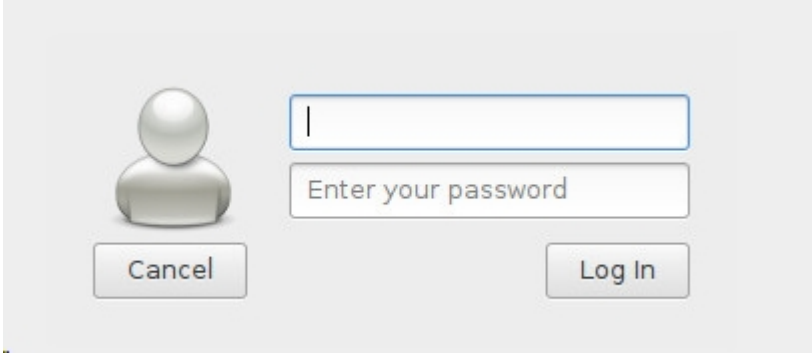
Now, you need to register the appliance.

Registering UDP Cloud Direct Virtual Appliance

Once the Virtual Appliance is installed and powered on, you need to register the UDP Cloud Direct Virtual Appliance with the Arcserve® Business Continuity Cloud.

Follow these steps:

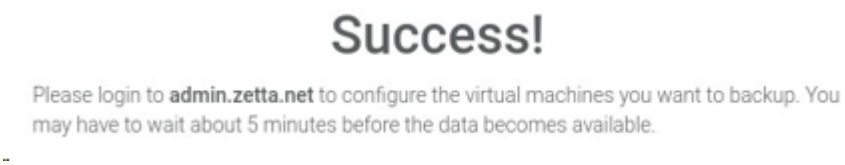
1. In the VMware vSphere Web Client, navigate to the *Console* tab for the virtual appliance.



2. Enter the default user name *zetta*, the default password *zettazetta*, and click **Log In**.
3. Enter the user account credentials (email/password) of a user created under your account that leverages the virtual appliance, and then click **Continue to vCenter Configuration**.

4. Enter your vCenter Server address, vCenter Username, and vCenter Password, and then click **Complete Configuration**.

You should get confirmation about successful completion of registration. Also, within 5 minutes data becomes available in the UDP Cloud Direct Portal.



5. **Optional step:** You can click *Change Appliance Password* to change the password for your UDP Cloud Direct Virtual Appliance using your current default password.

You have registered the UDP Cloud Direct Virtual Appliance successfully. A policy is created for the Appliance, the policy name is *<System Name> + Policy*. Now, to complete configure the appliance.

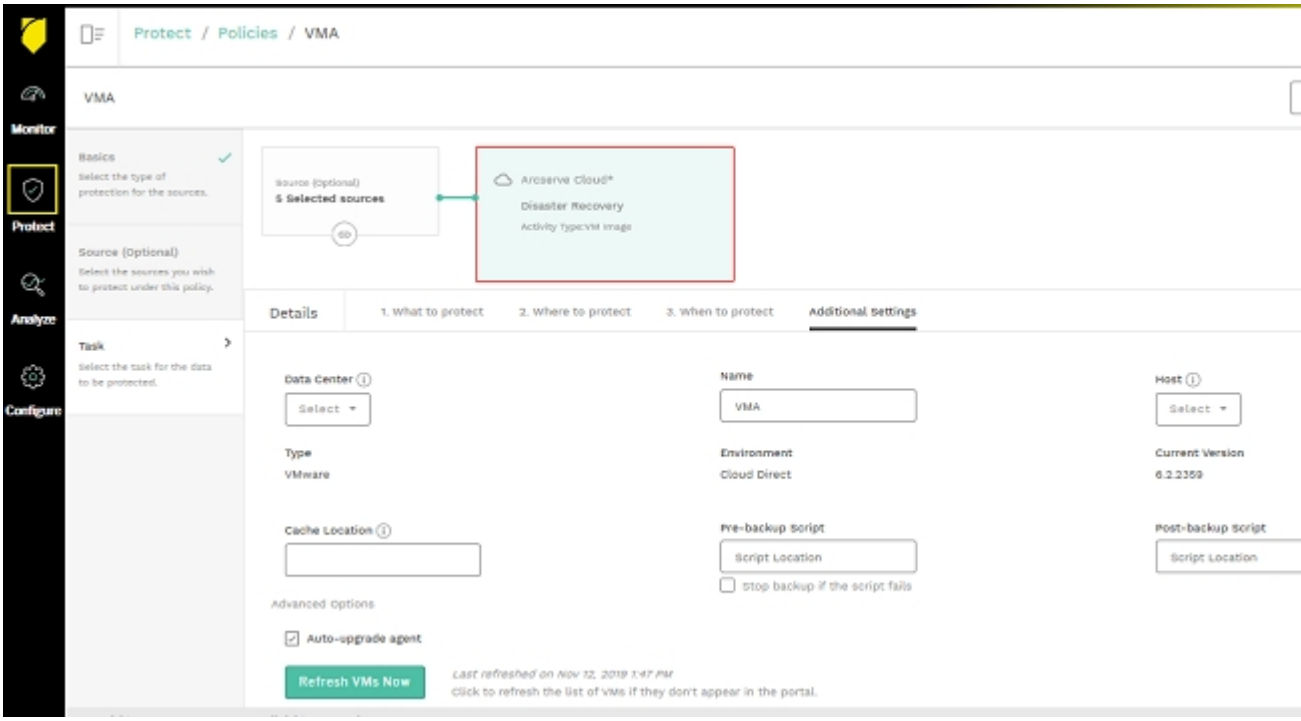
Configure UDP Cloud Direct Virtual Appliance

You can configure a virtual appliance after completion of registration to the Console. To configure, you must add the virtual machines as a source. For more information, see Add a source. Then, you can configure the settings as required.

Follow these steps:

1. From the displayed list at Configure > Infrastructure > Hypervisors, click name of the desired Virtual Appliance or from Protect > Policies, modify the Appliance policy.

   The virtual appliance policy modification page is displayed.



2. Click the **Destination** tab and perform the following steps:

   a. From the **Where to protect**, specify the desired destination where you want to store the data.

   b. From the **When to protect** tab, assign a backup schedule to run.

   Note: You can also add a Throttle Schedule to restrict bandwidth usage.

   If you select a Disaster Recovery destination, recovered resources are created for all added sources in the policy.

3. From the **Additional Settings**" tab, you can add/update the information of the following fields and click **Save**:

Data Center / Host

Default set to None. When a value is set, only virtual machines from this Data Center / Host is protected.

Note: Verify that VMs outside are already disabled.

Name

Refers to the System name provided during registration. You can modify if required.

Cache Location

Enter the location where the cache is stored. The Cache Location locally stores cache to optimize transfer performance. It roughly totals 1% of the data set. If free disk space is a concern, provide an alternate location for the cache.

Pre-backup Script

Enter the location of the script that executes before the backup job runs and to stop the backup when script fails, check the Stop backup if the script fails (Optional) checkbox

Post-backup Script

Enter the location of the script that executes after the backup is completed.

Auto-upgrade agent

Refers to the agent. Enabled by default, lets you automatically upgrade the agent in Virtual Appliance.

Auto-sync new VMs

Lets you sync the VMs from vCenter daily. The option is disabled by default. To manually sync the VMs, you can click **Refresh VMs now**.

The configuration of virtual appliance is complete.

Delete UDP Cloud Direct Virtual Appliance

You can delete an existing UDP Cloud Direct virtual appliance.

Considerations:

- If a recovered resource is running for an enabled virtual machine, you cannot delete the virtual appliance.
- All the enabled virtual machines are also deleted.

Follow these steps:

1. Navigate to Configure > Infrastructure > Hypervisors.

   All the added virtual appliances are displayed.
2. From the displayed list, click **Action** drop-down option for the desired virtual appliance.

   The option to delete appear.
3. Click **Delete**.

   A confirmation message appears.
4. Click **Yes** to confirm.

   The virtual appliance is deleted.

Set up UDP Cloud Direct Agent for Hyper-V

Perform a Hyper-V integration to protect data that resides on VMs of Hyper-V.

Follow these steps:

1. Navigate to the **Protect** screen and click **Download Cloud Direct Agent**.
2. Copy the downloaded file and paste the file to the Hyper-V machine.
3. Run the file as per the set-up instructions to complete the installation of Cloud Direct Agent.
4. After installing Cloud Direct Agent, provide your cloud account details in the registration window, to add Hyper-V to cloud console.

   The Hyper-V appears in the **Machines** field of the **Protect** Screen. The **Backup VMs** options may appear after sometime.
5. Scroll towards the far right of the source node and select **Backup VMs** option from the contextual view.

The Hyper-V gets highlighted in red in the source list and appears in the **Hypervisors** field of the **Configure** screen. The Hyper-V may appear in the **Hypervisors** field after sometime.

Subsequently, a default policy gets created in the **Polices** field of the **Protect** screen.

6. Add VMs to the Hyper-V by following one of the below methods:

   Using the Configuration Screen

   1. Navigate to the **Hypervisors** field and select a Hyper-V name to proceed to the Edit Policy page.
   2. Click the **Sources** field and click **Select Sources** to view the VMs residing on the Hyper-V.
   3. Select the checkboxes with the VM names which you want to backup and click Add Sources.

   Using the Protect Screen

   1. Navigate to the **Policies** field and select a policy that has the Hyper-V name.
   2. Click the **Sources** field and then click **Select Sources** to view the VMs residing on the Hyper-V.
   3. Select the checkboxes with the VM names which you want to backup and click Add Sources.
   4. Click the **Destinations** field and then click the Activity Type: VM Image box and edit the following fields as per your requirement:
      - Where to protect
      - When to protect
      - Additional settings
   5. From the **Additional Settings** tab, do the following:
      - For **Cache Location**, enter the location where the cache is stored. The Cache Location locally stores cache to optimize transfer performance. It roughly totals 1% of the data set. If free disk space is a concern, provide an alternate location for the cache.
      - For **Pre-backup Script**, enter the location of the script that executes before the backup job runs.
      - (Optional) To stop the backup when script fails, check the **Stop backup if the script fails** checkbox.

- For **Post-backup Script**, enter the location of the script that executes after the backup is completed.

Note: After an Agentless backup is performed, the operating system information does not appear. To display the operating system information, install the Integration Services in the guest OS and power-on the VM.

7. (Optional) If a new VM is added under Hyper-V, click **Refresh VMs Now** while modifying the policy to make them available in cloud console. Follow step 6 to manually add the VMs to Cloud Console.

   Hyper-V integration to protect data that resides on VMs of Hyper-V is now complete.

Configuring Source Group

Source Groups refer to the groups that contain multiple sources. Using the feature, you can maintain groups of specific type of sources. The Source Group screen displays the existing groups and provides option to create or delete a group. You can also use the search option to find a group.

Key Highlights:

- Search a group: From the Source Group screen, you can search a group using the **Search** option.
- View source group details: View details related to a source group. For example, Name of group, Total Assigned Sources, Protected Sources and Not Protected Sources.
- Delete a source group: Use the drop-down option available for every source group to delete a group.

For list of global and individual actions, view following links:

- How to Perform Common Individual and Global Actions
- How to perform individual actions for Cloud Hybrid
- How to perform global actions for Cloud Hybrid
- How to perform individual actions for Cloud Direct
- How to perform global actions for Cloud Direct

What's Next!

- Create a Source Group
- Assign Sources to a Source Group

Create a New Source Group

From the Source Group feature, you can create multiple groups for sources.

Follow these steps:

1. From the Source Group screen, click **Create Group**.

   Create Group dialog is displayed.

2. Enter a unique name as the **Group Name**.
3. Click **Create**.

   The new source group is visible on the Source Groups screen.

Assign Sources to a Source Group

You can assign available sources to the source groups. Simply, open a source group and assign relevant sources.

Follow these steps:

1. From the Source Group screen, click name of a source group.

   The screen of that source group displays related details.

2. Click **Add Sources to Group**.

   Add Sources to Group screen appears displaying the list of available sources

3. Select the checkbox of sources to add.

   Selected field on top shows the number of sources you opted to add.

4. Click **Add Selected Sources**.

   The source group name screen displays the number of added selected sources.

From Actions drop-down list, you can select to remove some sources from the source group. To remove one or more sources, follow these steps:

1. Select the checkbox of desired sources.
2. Click **Remove from Group** option available in **Actions** drop-down list.

   A confirmation dialog appears.

3. Click **Confirm** to remove.

Configuring Access Control

The feature lets you manage users. You can add a new user and also perform specific action for existing users.

Note: Using this option, you cannot manage your own details. You can only manage the users that you add. To reset your password, navigate to User Profile.

What's next!

- Manage User Accounts
- Manage Roles

Manage User Accounts

Using User Accounts feature, you can manage users. You can add a new user and also perform specific action on existing users. For example, resending verification email, reset a password, and delete a user. You can also use the Manage Saved Search option to perform collective action on users. Using the search option, you can find user according to the selected filters - such as Status, Is blocked and role - and save the search results. For more information, view how to manage saved search.

Notes:

- Using this option, you cannot manage your own details. You can only manage the users that you add. To reset your password, navigate to User Profile.
- To enable two-factor authentication (2FA) requirement for the users that you have added, see How to Enable 2FA Requirement at Organization Level.
- To disable two-factor authentication (2FA) requirement for the users that you have added, see How to Disable 2FA Requirement at Organization Level.

For list of global and individual actions, view following links:

- How to Perform Common Individual and Global Actions
- How to perform individual actions for Cloud Hybrid
- How to perform global actions for Cloud Hybrid
- How to perform individual actions for Cloud Direct
- How to perform global actions for Cloud Direct

What's next!

- View and Update User Account
- Add a User

How to View and Update User Account

Arcserve® Business Continuity Cloud lets you view and perform multiple actions on user accounts. From User Accounts screen, you can search users, view details and perform multiple actions on the existing accounts.

Key Actions Performed on User Accounts:

- **Update User Name:** You can edit first name and last name of user.
- **Search User Accounts:** Enter a search term or use desired filters in the search box to search an account. You can save the search and also manage saved search.
- **View User Account Details:** The User Accounts screen displays all the added user accounts with specified details set using the icon  . For example, Email, role, last logged on, Is Blocked, and so on.
- **Delete User Account:** Select multiple accounts and select delete from drop-down option of **Actions** to delete multiple accounts together. To delete one user account, click the drop-down arrow placed in user account details and click **Delete**. A Confirmation dialog is displayed. Click **Confirm** to delete.
- **Reset Password:** This option appears for those existing users whose status displays verified or **Is Blocked** status is displayed as false. Clicking **Reset Password** option from the drop-down list of one user results in a Confirmation dialog. Click **Send Email** to confirm reset password and a link is sent to the registered email ID of selected user.

  Note: After sending the Reset Password link, the user cannot log into the Console using the old password.
- **Reset Two Factor:** To disable two-factor authentication for a particular user, select the **Reset Two Factor** option from the Action drop-down list. The confirmation message appears asking you to disable two-factor authentication. Click **Reset User Two Factor** to confirm.

  Note: After the two factor is reset, 2FA gets disabled.
- **Resend Verification Mail:** The option appears for those users who are added but not verified. Click **Resend Verification Email** from the drop-down list of a user. A confirmation message informs that the email was sent to the email ID of the selected user.
- **Add a user:** From the User Accounts screen, click the option to add a user. For details, view How to add a user.

How to Add a User

From the User Account screen, you can add a new user and assign role.

Follow these steps:

1. Click **Add User**.

   Add User dialog is displayed.

2. Enter the following details:

   - **First Name** and **Last Name**: Enter full name of user
   - **Email Address:** Enter the email address of user. Email address cannot be reused for other user. The verification email is sent to the provided email ID. To get verified, the new user needs to click the activation link sent to the provided email. After successful verification, the user is assigned a role and then only user can perform any action. Without clicking the activation link shared in the verification email to create password, the user remains unverified and cannot login to the Console.
   - **Role:** Select a role to assign the new user. For example, Admin.

3. Click **Add User**.

   The Add User dialog closes and the new user is displayed at the User Account screen.

Manage Roles

From Roles screen, you can view details about the active role.

Key Highlights:

- Expand the name of role to view permissions assigned to the role.
- View number of users who have the role assigned.
- View description about a role.

Configuring Entitlements

Arcserve® Business Continuity Cloud lets you manage your entitlements directly from the Console. Click Entitlements and view details such as Account Summary, Entitlements for Arcserve Cloud, and Cloud Hybrid.

Cloud Direct Trial Period:

- A Cloud Direct Trial period lasts 15 days. After the end of trial period, all the Cloud Direct policies are disabled and no backups run.
- After 30 days of trial expiry date, the Cloud Direct resources (For example: Sources, Destinations, and Policies) of the organization is removed from the console.

Cloud Hybrid Trial Period:

- A Cloud Hybrid Trial period lasts 15 days. After the end of trial period, all the Cloud Hybrid policies are disabled and no backups run.
- After 30 days of trial expiry date, the Cloud Hybrid resources (For example: Sources, Destinations, and Policies) of the organization are removed from the console.

From the screen, you can also activate new order.

Follow these steps:

1. From the Entitlements screen, click **Activate New Order**.

   Activate New Order dialog is displayed.

2. Enter the **Order ID** and **Fulfilment Number**.

   Details of both must belong to the same order.

3. Click **Activate**.

   A confirmation dialog provides the status.

Configuring Organization Branding

Branding allows you to customize details about your organization that customers generally require. For example, update emails, legal contacts, and Branding message that appear during login.

Follow these steps:

1. From Arcserve® Business Continuity Cloud, click **Branding**.

   Branding screen appears with three tabs.

2. Click the tab **Your Brand** to add or update available options. For example,

   - Provide the description about Name and Portal URL/Hostname of your organization.
   - Select **Logo & Color**.

     Note: Logo is displayed in your brand page. Default logo is of Arcserve. The Primary and secondary colors indicate the Borders of the Console.

3. Click the tab **Emails** to configure details of organization, Support numbers, Social media links, Support emails, legal details such as Contact Us, notice, privacy and copyright information.

4. Click **Save Changes**.

   The login tab is enabled only if portal URL / Hostname is verified.

5. Click the tab **Login** to update Logo or use the existing logo. You can also provide the Branding Message that appears on login page.

   Note: The Login tab is visible only when **Portal URL** is provided for the tab, Your Brand.

6. Click **Save changes** after updating detail in the Login tab.

   Branding details are updated.

Chapter 4: Using Arcserve® Business Continuity Cloud as MSP Administrator

MSP administrator manages Arcserve® Business Continuity Cloud for MSP and MSP-based organizations.

This section contains the following topics:

Dashboard

After logging into Arcserve® Business Continuity Cloud, you land on the Console dashboard where you can view multiple common options and the details of Monitor feature. From the Dashboard, you can change password, update user details, view details to contact support, view important messages and log out.

Dashboard provides the following options:

- **Arcserve Icon:** Click on the Arcserve icon, placed on the top-left corner, and return to dashboard from anywhere in the Console.
- **Help Icon:** The Help icon on top-right takes you to the **Support** page where you can opt from multiple options to contact Arcserve and view Online help for the Console.
- **Alert Icon:** The exclamation mark icon on top-right displays messages from the Console for your consideration. The messages are categorized as **Critical**, **Warning** or **Information**. You can Acknowledge the messages and take action when required. For more details, view How to Manage Alerts.
- **User Login Icon:** The icon on top-right corner displays the profile picture of the logged-in user. The icon provides option to log out from Cloud Console and update user profile of the logged-in user.

Using User Profile, you can make two updates:

- **Update Contact Information:** From **My Profile** screen, you can update your contact details and upload photo. Click **Save Changes** after making updates.
- **Change Password:** Provide a new password and click **Update Password**.
- **Two-Factor Authentication:** Provide the current password, and then do one of the following:
  - To enable two-factor authentication, click **Enable Two Factor Authentication**.
  - To disable two-factor authentication, click **Disable Two Factor Authentication**.
  - To generate two-factor codes, click **Generate Two Factor Codes**.

Monitor

After logging into Arcserve® Business Continuity Cloud, you land on the Console dashboard where Monitor displays the details of your product using multiple wizards. From the Monitor, you can perform the following options:

- **View Summary:** Monitor displays summary of customer, usage, and source for the organization.
  - **Customer Summary:** Displays the count of Total customers and the count of customers with Failed and Success status based on the job result of last backup.
  - **Usage Summary across customers:** Displays the usage summary of customers according to the licensed capacity for Cloud Direct or Cloud Hybrid.
  - **Source summary across customers:** Displays the count of sources of all customers according to the status. For example, protected, not protected and offline.
- **View Details as Graphs:** For better monitoring of key details, Monitor displays graphical view of multiple fields. For example:
  - **Backup Job Summary:** Displays the last 24 hours Backup Job count for Finished, Canceled, or Failed status. Hover over the graph to view the percentage for each status.
  - **Recent 10 Jobs in Progress:** Displays recent 10 jobs in progress, supports view log or cancel job action for all *in progress* job. Clicking **View all jobs** link leads you to the Jobs screen.
  - **Top 10 Sources:** Display top 10 sources per specific condition. Supports selected Backup Job Status, Events, Job Durations, and Data Transferred.
  - **Top 10 Polices:** Displays top 10 policies and group by Job status as Finished, Failed, Canceled, or Active.
  - **View Top 10 Customers:** Helps you monitor Top 10 customers of MSP user.
  - **Usage Trend for Cloud Direct Volumes:** Displays Usage Trend for Cloud Direct Volumes by Full backup data and group by volume name.
  - **Usage Trend for Cloud Hybrid Stores:** Displays Usage Trend for Cloud Hybrid Stores and group by Cloud Hybrid Store name.

- **Data Transfer Summary For Cloud Direct Volumes:** Displays Data Transfer Summary for Cloud Direct Volumes and group according to Data Processed, Data Transferred, and Data Written.
- **Dedupe Savings Trends For Cloud Hybrid Stores:** Displays Dedupe Savings Trends For Cloud Hybrid Stores and group by Source Data and Dedupe Savings size.

- **View Cloud Hybrid Details:** View usage trend and dedupe savings trend for Cloud Hybrid Stores. Hover over the graph to view details.
- **Expand or Collapse widgets:** Use the icon placed above a displayed widget to expand or collapse.

Protect

MSP Admin can protect customer accounts. From the customer accounts MSP Admin can perform the following actions:

- Search and View details of all customer accounts
- Add and Modify a new customer account

How to Search, View, and Perform Multiple Actions on Customer Account

The Customer accounts screen provides multiple options. For example, view details, modify customer account, and perform multiple actions.

Search an account: From the search bar, find customer accounts using the name of the customers.

View account details: The customer accounts screen displays the list of all available customer accounts. For each account, view details such as Customer Name, Status, Account State, Total Sources, Product Usage, Added by and Added on.

View Count of Accounts: On the top-right corner of the page, **Total Customer Accounts** displays the number of customer accounts added.

View Count of Accounts Suspended: On the top-right corner of the page, **Total Customer Accounts Suspended** displays the number of customer accounts suspended.

Add a Customer Account: From the screen, you can add a customer account. For more information, see how to add customer account.

Perform Multiple Actions: Every account has a drop-down of actions at the end. From the drop-down option, you can select one of the following options:

- **Set usage threshold:** Set a threshold of usage for specific customer account in the Set Usage Threshold dialog. Select the Usage Threshold and click **Save**. You can select limit in TB, GB, and PB.
- **Assign MSP Account Admin:** Allocate an MSP account admin to the customer account. From **Assign Admins to customer** dialog, select one or more admins, click **Add** and then click **Assign**.
- **View as End-User Admin:** Use the icon placed before the name of customer account or from the drop-down option, click to switch role to view customer account.
- **Delete:** Remove the customer account from organization. Clicking **Delete** opens a Confirmation Message to Delete Customer Account. Click **Delete** in the message to remove the customer account.
- **Suspend:** MSP Admin is allowed to suspend the customer account. To suspend, from the **Action** drop-down list, click **Suspend**. For more information, see Suspend Organization.

- **Enable:** MSP Admin is allowed to resume the suspended customer account. To Resume, from the **Action** drop-down list, click **Enable**. For more information, see Enable Organization.

How to Add and Modify a Customer Account

From the customer account screen, you can add or modify a customer account.

Adding the customer account is simple.

Follow these steps:

1. Click **Add Customer Account**.
2. Enter a name in the dialog that opens.
3. Click **Add Customer**.

The new customer account is displayed on customer accounts screen. You can view details and perform multiple actions on the customer accounts. For more information, view How to Search, View, and Perform Multiple Actions on Customer Account.

You can also modify the details of a customer account.

Follow these steps to modify a customer account:

1. From the Customer Accounts dashboard, click the name of a customer account.

   The screen of any specific customer account displays two tabs: Information and Metrics.
2. From the **Information** tab, you can view General information and make the following updates:
   - Modify the name of the customer.
   - Assign an admin to the customer account. Click **Assign Admin**, select an admin from the **Assign Admin to customer** dialog, click **Add** and then click **Assign**.
   - The assigned admins are displayed on the Information tab of that customer account.
   - Unassign an admin from the customer account. To unassign an admin, you need to click **Unassign account** from the drop-down option against the name of an admin.
   - After making desired updates, click **Save Changes** on the top of screen.
3. From the **Metrics** tab, view Capacity Usage Trends and Protection Summary of that account. You can select different durations from the respective drop-downs displaying time duration.

Analyze

MSP Administrator can analyze jobs, logs and reports.

- Analyze Jobs
- Analyze Logs
- Analyze Reports

Analyzing Jobs

Displays complete list of jobs with the details that you can customize.

Key Highlights

- The search bar helps you find a job according to the selected filters. For example, status, job type, date range or protection policy.
- You can save the search also for future usage.
- Manage Saved Search option lets you manage a search if you have saved. For more information, view how to manage saved search.
- All the jobs display details that you can customize by using the Settings icon. Jobs are divided into multiple categories based on status. For example, Jobs in Progress, Failed Jobs, Canceled Jobs, and Successful Jobs.
- View Job description, such as Name of job, type of job, status of job, policy associated with source, destination of recovery point, duration, start and end time of job. You can also view the job description from the Jobs tab on the screen of a source.
- For every job, you can **view log**. Click the drop-down option placed at the end of every row of a job to view log of that job.
- You can also **Cancel** a job that is in progress.

  For list of global and individual actions, view following links:

  - How to Perform Common Individual and Global Actions
  - How to perform individual actions for Cloud Hybrid
  - How to perform global actions for Cloud Hybrid
  - How to perform individual actions for Cloud Direct
  - How to perform global actions for Cloud Direct

Analyzing Logs

The log tab displays all activity logs for the protected nodes, destination servers, data stores, and policies. You can view logs and apply various filters such as severity, logs generated from the machine, job type, and log content. You can also Export logs. Message ID provides a hyperlink to access detailed documentation. Click the hyperlink in the MessageID column to view the description and solution for that message. On the log screen, Message IDs are displayed only for Replication IN jobs.

Export Logs: From the Log screen, you can export the logs to your Inbox. Click **Export** from the top of Log screen and the log is sent to your registered email ID. In your inbox, find the email from Arcserve Cloud Support email with the subject Log Export and click **Download Export** in the email to download log as .csv file.

Search Logs: You can search the activity logs using a combination of the available filters or one of the following options and clicking **Search**:

- Select **Severity** types to view all the logs related to the selected type.
- Select **Job Type**.
- Select **Date Range**.
- Select **Generated From** location.
- Enter message term in the Search box.

Analyzing Alert Reports

Use Arcserve® Business Continuity Cloud to analyze alerts separately or together based on the alert type.

From the list of alerts, you can view alert details such as Alert Name, Alert Type, Report for, Created on, Last Generated, and Recipients.

From the Alerts screen, you can perform following actions:

- Create a New Alert Report
- Edit an Alert Report

Create a New Alert Report

Using **Create Alert**, you can add new alert report. The alert report is sent as a link to the email and additional recipients, if added. The **Create Alert** report wizard is required to create new report. The wizard appears when you click **Create Alert** on the alerts page.

Follow these Steps:

1. From the Analyze screen, click **Alerts** tab.

   The Alerts screen appears.

2. From the Alerts screen, click **Create Alert**.

   The Create Alert wizard appears.

3. From the **Create Alert** wizard, from **Alert Type**, select one of the options.
4. For Alert Name, enter a unique name for your new alert report.
5. Select one of the following options:
   - **Report all Organizations:** Lets you generate report from all available Organizations.
   - **Report selected Organizations:** Lets you generate report only from the selected Organizations. If you select this option, from the drop-down option, select Organizations, and then click **Add**. To select organizations, repeat the action.
6. (Optional) To share your report with others, enter email addresses of one or more recipients, and then click **Add**.
7. Click **Create**.

   A confirmation dialog appears that displays the successful generation of the alert report.

The Alert Report screen contains the success report. When the backup is completed, an email is sent to the logged in user and other recipients, if any.

Edit an Alert Report

You can edit an Alert Report in the Alerts page.

Follow these steps:

1. From the Analyze screen, click **Alerts**.

   The Alerts – Reports screen displays a List of reports. From the list, click the name of an Alert Report or use the drop-down option to select the report, and then click **Edit**.

   The Edit Report Settings screen appears.

2. From the screen, select one of the options to specify the Organizations:
   - **Report all Organizations:** Lets you edit reports from all available Organizations.
   - **Report selected Organizations:** Lets you edit reports only from the selected Organizations. If you select this option, from the drop-down option, select Organizations, and then click Add. To select Organizations, repeat the action.
3. To share your report with others, enter email addresses of one or more recipients, and then click **Add**.
4. Click **Save Changes**.

   The report is modified.

Analyzing Reports

Using the Console, you can view four types of reports: Backup Jobs, Recovery Jobs, Data Transfer, and Capacity Usage. Search bar lets you find a report using filter criteria such as Generated on, Scheduled for, and Date Range. You can create a report or view reports about Backup and Recovery Jobs, Data Transfer, and Capacity Usage. You can also export reports as .csv file.

- Create Report
- View Reports
- Manage Report Schedules
- Export report
- Edit a report schedule

How to View a Report

You can manage schedules of all the report using Manage Report Schedules. Under Analyze>Reports, click Manage Report Schedules and you can view list of all reports. From the screen, you can perform the following actions:

- **Search:** To search reports, either provide a report name in the search bar or use filters of **Scheduled for** and **Report Type**.
- **View details:** The list of report provides complete details about every report. For example, Report Name, Report Type, Report for, Scheduled For, Created by, Created on, Last Generated. You can click a Report Name to edit settings of the report.
- **Global Actions:** When you select check box of one or more report names, in the top bar **Selected** shows the number of check boxes selected and **Actions** option is enabled to help you perform collective action on selected reports. For example, **Delete** all selected reports or use **Generate Now** to prepare a copy of all selected reports.
- **Individual Actions:** On a specific report, you can perform the following individual actions:
  - **Edit Report:** From the drop-down option placed at the end of a report, when you click **Edit**, the dialog **for Edit Report Settings** appears. Make required modifications and click **Save Changes**. For more details, view how to edit a report schedule.
  - **Generate Now:** From the drop-down option placed at the end of a report, when you click **Generate Now**, an instance of that report is created and appears immediately in the list of reports.
  - **Delete A Report:** From the drop-down option placed at the end of a report, when you click **Delete Report**, a confirmation dialog appears. Click **Confirm** to delete the report.

    Note: While deleting report as individual or global action, you can also delete all report instances created by a report schedule. From the confirmation message, select the check box of **delete the report instances** also.

To view details of specific reports, click on one of the following report types:

- Backup Jobs
- Policy Tasks

- Recovery Jobs
- Data Transfer
- Capacity usage

Report for Backup Jobs

From the console, click Backup Jobs below Reports to reach the screen that lets you view summary of all the backup jobs. You can also search the source using the filters of Date Range, Protection Policy, and Destination. Using multiple filters is allowed. Click icon of Manage Saved Searches to select the option that you want to view in report.

Key Highlights:

- From the screen, you can Create Report and Export Report as .csv file.
- Hover over the chart to view percentage of Failed, Finished, and Canceled jobs.
- View top 10 sources and filter according to Backup Job Status, Events, Jobs Duration or Data Transferred.
- Hover over the graph to view classification of Finished, Failed and Canceled jobs.
- View **Details** of all backup jobs from the table.

Report for Policy Tasks

To view the policy tasks details of completed backup jobs, go to **Analyze** > **Policy Tasks**.

Click **Policy Tasks** to view the summary of the policy tasks of completed backup jobs. You can search the source using multiple filters such as Date Range, Protection Policy, Destination, and Organizations. On the top-right corner of the **Policy Tasks** page, click **Manage Saved Searches** and select an option that you want to view in the report.

Key Highlights

- From the screen, to create and export report as a .csv file, click **Create Report** and **Export Report** respectively.
- Hover over the chart to view the percentage of Finished, Failed, and Canceled jobs.
- Apply filters to view Top 10 Sources such as Events and Job Duration.
- Hover over the graph to view classification of Finished, Failed, and Canceled jobs.
- From the table, view Details of all policy tasks for completed backup jobs.

Report for Recovery Jobs

From the Console, click Recovery Jobs below Reports to reach the screen that lets you view summary of all the jobs restored. You can also search the source using the filters of Date Range, Destination, and Organization. Click icon of Settings to select the option that you want to view in report.

Key Highlights:

- Hover over the chart to view percentage of Failed, Canceled, and Finished jobs.
- View top 10 sources and filter according to Recovery Job Status, Events, Jobs Duration or Data Transferred.
- Hover over the graph to view classification of Finished, Failed and Canceled jobs.
- View **Details** of all recovery jobs from the table.
- Export the reports as CSV file.
- Create reports for individual reports for all roles.
- Manage saved search. For more information, view how to manage saved search.

Report for Data Transfer

From the console, click Data Transfer below Reports to reach the screen that lets you view summary of data transfer. You can also search the source using the filters of Date Range.

Key Highlights:

- Hover over the chart to view data processed, data transferred and data written on a specific date.
- Hover over the graph to view classification of Finished, Failed and Canceled jobs.
- View **Details** of all data transfer from the table.
- Export the reports as CSV file.
- Create reports for individual reports for all roles.
- Manage saved search. For more information, view how to manage saved search.

Report for Capacity Usage

From the console, click Capacity Usage below Reports to reach the screen that lets you view usage trends and dedupe savings trend. You can also search the destination using the filters of Date Range, and Destination.

Key Highlights:

- Hover over the chart to view usage trend and dedupe saving trend on different dates.
- View **Details** of capacity usage from the table.
- View details about all available destinations.
- Export the reports as CSV file.
- Create reports for individual reports for all roles.
- Manage saved search. For more information, view how to manage saved search.

Manage Report Schedules

You can manage schedules of all the report using Manage Report Schedules. Under Analyze>Reports, click Manage Report Schedules and you can view list of all reports. From the screen, you can perform the following actions:

- **Search:** To search reports, either provide a report name in the search bar or use filters of **Scheduled for** and **Report Type**.
- **View details:** The list of report provides complete details about every report. For example, Report Name, Report Type, Report for, Scheduled For, Created by, Created on, Last Generated. You can click a Report Name to edit settings of the report.
- **Global Actions:** When you select check box of one or more report names, in the top bar **Selected** shows the number of check boxes selected and **Actions** option is enabled to help you perform collective action on selected reports. For example, **Delete** all selected reports or use **Generate Now** to prepare a copy of all selected reports.
- **Individual Actions:** On a specific report, you can perform the following individual actions:
  - **Edit Report:** From the drop-down option placed at the end of a report, when you click **Edit**, the dialog **for Edit Report Settings** appears. Make required modifications and click **Save Changes**. For more details, view how to edit a report schedule.
  - **Generate Now:** From the drop-down option placed at the end of a report, when you click **Generate Now**, an instance of that report is created and appears immediately in the list of reports.
  - **Delete A Report:** From the drop-down option placed at the end of a report, when you click **Delete Report**, a confirmation dialog appears. Click **Confirm** to delete the report.

    Note: While deleting report as individual or global action, you can also delete all report instances created by a report schedule. From the confirmation message, select the check box of **delete the report instances** also.

Configure

Using the Console, you can configure Access Controls, Entitlements, and Branding for your organization.

What's Next!

- Configuring Access Control
- Configuring Entitlements
- Configuring Organization Branding

Configuring Access Control

The feature lets you manage users. You can add a new user and also perform specific action for existing users.

Note: Using this option, you cannot manage your own details. You can only manage the users that you add. To reset your password, navigate to User Profile.

What's next!

- Manage User Accounts
- Manage Roles

Manage User Accounts

Using User Accounts feature, you can manage users. You can add a new user and also perform specific action on existing users. For example, resending verification email, reset a password, and delete a user. You can also use the Manage Saved Search option to perform collective action on users. Using the search option, you can find user according to the selected filters - such as Status, Is blocked and role - and save the search results. For more information, view how to manage saved search.

Notes:

- Using this option, you cannot manage your own details. You can only manage the users that you add. To reset your password, navigate to User Profile.
- To enable two-factor authentication (2FA) requirement for the users that you have added, see How to Enable 2FA Requirement at Organization Level.
- To disable two-factor authentication (2FA) requirement for the users that you have added, see How to Disable 2FA Requirement at Organization Level.

What's next!

- View and Update User Account
- Add a User

How to View and Update User Account

Arcserve® Business Continuity Cloud lets you view and perform multiple actions on user accounts. From User Accounts screen, you can search users, view details and perform multiple actions on the existing accounts.

Key Actions Performed on User Accounts:

- **Update User Name:** You can edit first name and last name of user.
- **Search User Accounts:** Enter a search term or use desired filters in the search box to search an account. You can save the search and also manage saved search.
- **View User Account Details:** The User Accounts screen displays all the added user accounts with specified details set using the Settings icon. For example, Email, role, last logged on, Is Blocked, and so on.
- **Delete User Account:** Select multiple accounts and select delete from the drop-down option of **Actions** to delete multiple accounts together. To delete one user account, click the drop-down arrow placed in user account details and click **Delete**. A Confirmation dialog is displayed. Click **Confirm** to delete.
- **Assign Account:** For a user role of MSP Account Admin, you can select the user and click **Assign Account** from the drop-down option of **Actions** to assign one or more accounts to the user. From *Assign accounts to users* dialog, select one or more customers and click **Assign**.
- **Reset Password:** The option appears for those existing users whose status displays verified. Clicking **Reset Password** option from the drop-down list of selected user, results in a Confirmation dialog. Click **Send Email** to confirm reset password and a link is sent to the registered email ID of selected user.

  Note: After sending the Reset Password link, the user cannot login to Cloud Console with old password.
- **Reset Two Factor:** To disable two-factor authentication for a particular user, select the **Reset Two Factor** option from the Action drop-down list. The confirmation message appears asking you to disable two-factor authentication. Click **Reset User Two Factor** to confirm.

  Note: After the two factor is reset, 2FA gets disabled.
- **Resend Verification Mail:** The option appears for those users who are added but not verified. Click **Resend Verification Email** from the drop-down list of selected user. A confirmation message informs that the email was sent to the email ID of the selected user.

- **Add a user:** From the User Accounts screen, click the option to add a user. For details, view How to add a user.

How to Add a User

From the User Account screen, you can add a new user and assign role.

Follow these steps:

1. Click **Add User**.

   Add User dialog is displayed.

2. Enter the following details:

   - **First Name** and **Last Name**: Enter full name of user
   - **Email Address:** Enter the email address of user. Email address cannot be reused for other user. The verification email is sent to the provided email ID. To get verified, the new user needs to click the activation link sent to the provided email. After successful verification, the user is assigned a role and then only user can perform any action. Without clicking the activation link shared in the verification email to create password, the user remains unverified and cannot login to the Cloud Console.
   - **Role:** Select a role to assign the new user. For example, Admin.

3. Click **Add User**.

   Add User dialog closes and the new user is displayed at the User Account screen.

Manage Roles

From Roles screen, you can view details about the active role.

Key Highlights:

- Expand the name of role to view permissions assigned to the role.
- View number of users who have the role assigned.
- View description about a role.

Configuring Entitlements

Arcserve® Business Continuity Cloud lets you manage your entitlements directly from the Console. Click Entitlements and view details such as Account Summary, Entitlements for Arcserve Cloud and Cloud Hybrid.

Cloud Direct Trial Period:

- A Cloud Direct Trial period lasts 15 days. After the end of trial period, all the Cloud Direct policies are disabled and no backups run.
- After 30 days of trial expiry date, the Cloud Direct resources (For example: Sources, Destinations, and Policies) of the organization is removed from the console.

Cloud Hybrid Trial Period:

- A Cloud Hybrid Trial period lasts 15 days. After the end of trial period, all the Cloud Hybrid policies are disabled and no backups run.
- After 30 days of trial expiry date, the Cloud Hybrid resources (For example: Sources, Destinations, and Policies) of the organization are removed from the console.

From the screen, you can also activate new order.

Follow these steps:

1. From the Entitlements screen, click **Activate New Order**.

   Activate New Order dialog is displayed.

2. Enter the **Order ID** and **Fulfilment Number**.

   Details of both must belong to the same order.

3. Click **Activate**.

   A confirmation dialog provides the status.

Configuring Organization Branding

Branding allows you to customize details about your organization that customers generally require. For example, update emails, legal contacts, and Branding message that appear during login.

Follow these steps:

1. From Arcserve® Business Continuity Cloud, click **Branding**.

   Branding screen appears with three tabs.

2. Click the tab **Your Brand** to add or update available options. For example,

   - Provide the description about Name and Portal URL/Hostname of your organization.
   - Select **Logo & Color**.

     Note: Logo is displayed in your brand page. Default logo is of Arcserve. The Primary and secondary colors indicate the Borders of the Console.

3. Click the tab **Emails** to configure details of organization, Support numbers, Social media links, Support emails, legal details such as Contact Us, notice, privacy and copyright information.

4. Click **Save Changes**.

   The login tab is enabled only if portal URL / Hostname is verified.

5. Click the tab **Login** to update Logo or use the existing logo. You can also provide the Branding Message that appears on login page.

   Note: The Login tab is visible only when **Portal URL** is provided for the tab, Your Brand.

6. Click **Save changes** after updating detail in the Login tab.

   Branding details are updated.

Chapter 5: Using Arcserve® Business Continuity Cloud as MSP Account Administrator

MSP Account administrator manages Arcserve® Business Continuity Cloud for MSP-based organizations.

This section contains the following topics:

Dashboard

After logging into Arcserve® Business Continuity Cloud, you land on the Console dashboard where you can view multiple common options and the details of Monitor feature. From the Dashboard, you can change password, update user details, view details to contact support, view important messages and log out.

Dashboard provides the following options:

- **Arcserve Icon:** Click on the Arcserve icon, placed on the top-left corner, and return to dashboard from anywhere in the Console.
- **Help Icon:** The Help icon on top-right takes you to the **Support** page where you can opt from multiple options to contact Arcserve and view Online help for the Console.
- **Alert Icon:** The exclamation mark icon on top-right displays messages from the Console for your consideration. The messages are categorized as **Critical**, **Warning** or **Information**. You can Acknowledge the messages and take action when required. For more details, view How to Manage Alerts.
- **User Login Icon:** The icon on top-right corner displays the profile picture of the logged-in user. The icon provides option to log out from Cloud Console and update user profile of the logged-in user.

Using User Profile, you can make two updates:

- **Update Contact Information:** From **My Profile** screen, you can update your contact details and upload photo. Click **Save Changes** after making updates.
- **Change Password:** Provide a new password and click **Update Password**.
- **Two-Factor Authentication:** Provide the current password, and then do one of the following:
  - To enable two-factor authentication, click **Enable Two Factor Authentication**.
  - To disable two-factor authentication, click **Disable Two Factor Authentication**.
  - To generate two-factor codes, click **Generate Two Factor Codes**.

Monitor

MSP account administrator can view Customer Summary, Usage Summary across customers, and Source summary across customers.

- **View Summary:** Monitor displays summary of customer, usage, and source for the organization.
  - **Customer Summary:** Displays the count of Total customers and the count of customers with Failed and Success status based on the job result of last backup.
  - **Usage Summary across customers:** Displays the usage summary of customers according to the licensed capacity for Cloud Direct or Cloud Hybrid.
  - **Source summary across customers:** Displays the count of sources of all customers according to the status. For example, protected, not protected and offline.

    Note: Clicking on the hyperlinked status terms leads you directly to the respective detailed screen. For example, from **Source Summary**, clicking **Protected** leads you to the Sources screen that displays the list of protected sources.
- **View Details as Graphs:** For better monitoring of key details, Monitor displays graphical view of multiple fields. For example:
  - **Backup Job Summary:** Displays the last 24 hours Backup Job count for Finished, Canceled, or Failed status. Hover over the graph to view the percentage for each status.
  - **Recent 10 Jobs in Progress:** Displays recent 10 jobs in progress, supports view log or cancel job action for all *in progress* job. Clicking **View all jobs** link leads you to the Jobs screen.
  - **Top 10 Sources:** Display top 10 sources per specific condition. Supports selected Backup Job Status, Events, Job Durations, and Data Transferred.
  - **Top 10 Polices:** Displays top 10 policies and group by Job status as Finished, Failed, Canceled, or Active.
  - **Usage Trend for Cloud Direct Volumes:** Displays Usage Trend for Cloud Direct Volumes by Full backup data and group by volume name.

- **Usage Trend for Cloud Hybrid Stores:** Displays Usage Trend for Cloud Hybrid Stores and group by Cloud Hybrid Store name.
- **Data Transfer Summary For Cloud Direct Volumes:** Displays Data Transfer Summary for Cloud Direct Volumes and group according to Data Processed, Data Transferred, or Data Written.
- **Dedupe Savings Trends For Cloud Hybrid Stores:** Displays Dedupe Savings Trends For Cloud Hybrid Stores and group by Source Data or Dedupe Savings size.

- **View Cloud Hybrid Details:** View usage trend and dedupe savings trend for Cloud Hybrid Stores. Hover over the graph to view details.
- **Expand or Collapse widgets:** Use the icon placed above a displayed widget to expand or collapse.
- **View Top 10 Customers:** Helps you monitor details of top 10 customers.

Protect

MSP account administrator can protect customer accounts of sub-organization.

- Search, View and Perform Multiple Actions on Customer Account
- How to Modify a Customer Account

Notes:

- To enable two-factor authentication (2FA) requirement for the tenants through impersonation view, see Enabling 2FA Requirement through Impersonation View.
- To disable two-factor authentication (2FA) requirement for the tenants through impersonation view, see Disabling 2FA Requirement at Organization Level.

How to Search, View and Perform Multiple Actions on Customer Account

The Customer accounts screen provides multiple options. For example, view details, modify customer account, and perform multiple actions.

Search an account: From the search bar, find customer accounts using the name of the customers.

View account details: The customer accounts screen displays the list of all available customer accounts. For each account, view details such as Customer Name, Status, Account State, Total Sources, Product Usage, Added by and Added on.

View Count of Accounts: On the top-right corner of the page, **Total Customer Accounts** displays the number of customer accounts added.

View Count of Accounts Suspended: On the top-right corner of the page, **Total Customer Accounts Suspended** displays the number of customer accounts suspended.

Perform Multiple Actions: Every account has a drop-down of actions at the end. From the drop-down option, you can select one of the following options:

- **Set usage threshold:** Set a threshold of usage for specific customer account in the Set Usage Threshold dialog. Select the Usage Threshold and click Save. You can select limit in TB, GB, and PB.
- **View as End-User Admin:** Use the icon placed before the name of customer account or from the drop-down option, click to switch role to view customer account.
- **Suspend:** MSP Account Admin is allowed to suspend the customer account. To suspend, from the **Action** drop-down list, click **Suspend**. For more information, see Suspend Organization.
- **Enable:** MSP Account Admin is allowed to resume the suspended customer account. To Resume, from the **Action** drop-down list, click **Enable**. For more information, see Enable Organization.

How to Modify a Customer Account

MSP Account administrator can modify a customer account. The administrator can modify details related to a customer account but cannot unassign an admin from the customer account.

Follow these steps:

1. From the Customer Accounts dashboard, click the name of a customer account.

   The screen of a customer account appears displaying two tabs: Information and Metrics.

2. From the **Information** tab, **Modify** the name of the customer and click **Save Changes** at the top of screen.

3. From the **Metrics** tab, modify time duration.

   You can select different durations from the respective drop-downs displaying time duration.

Analyze

MSP account administrator can analyze jobs and logs.

Analyzing jobs

Analyzing logs

Analyzing Jobs

Displays complete list of jobs with the details that you can customize.

Key Highlights

- The search bar helps you find a job according to the selected filters. For example, status, job type, date range or protection policy.
- You can save the search also for future usage.
- Manage Saved Search option lets you manage a search if you have saved. For more information, view how to manage saved search.
- All the jobs display details that you can customize by using the Settings icon. Jobs are divided into multiple categories based on status. For example, Jobs in Progress, Failed Jobs, Canceled Jobs, and Successful Jobs.
- View Job description, such as Name of job, type of job, status of job, policy associated with source, destination of recovery point, duration, start and end time of job. You can also view the job description from the Jobs tab on the screen of a source.
- For every job, you can **view log**. Click the drop-down option placed at the end of every row of a job to view log of that job.
- You can also **Cancel** a job that is in progress.

  For list of global and individual actions, view following links:

  - How to Perform Common Individual and Global Actions
  - How to perform individual actions for Cloud Hybrid
  - How to perform global actions for Cloud Hybrid
  - How to perform individual actions for Cloud Direct
  - How to perform global actions for Cloud Direct

Analyzing Logs

The log tab displays all activity logs for the protected nodes, destination servers, data stores, and policies. You can view logs and apply various filters such as severity, logs generated from the machine, job type, and log content. You can also Export logs. Message ID provides a hyperlink to access detailed documentation. Click the hyperlink in the MessageID column to view the description and solution for that message. On the log screen, Message IDs are displayed only for Replication IN jobs.

Export Logs: From the Log screen, you can export the logs to your Inbox. Click **Export** from the top of Log screen and the log is sent to your registered email ID. In your inbox, find the email from Arcserve Cloud Support email with the subject Log Export and click **Download Export** in the email to download log as .csv file.

Search Logs: You can search the activity logs using a combination of the available filters or one of the following options and clicking **Search**:

- Select **Severity** types to view all the logs related to the selected type.
- Select **Job Type**.
- Select **Date Range**.
- Select **Generated From** location.
- Enter message term in the Search box.

Chapter 6: Using Arcserve® Business Continuity Cloud as End-User Administrator

The end-user administrator manages Arcserve® Business Continuity Cloud for end user of MSP.

This section contains the following topics:

User Profile

After logging into Arcserve® Business Continuity Cloud, you land on the Console dashboard where you can view multiple common options and the details of Monitor feature. From the Dashboard, you can change password, update user details, view details to contact support, view important messages and log out.

Dashboard provides the following options:

- **Arcserve Icon:** Click on the Arcserve icon, placed on the top-left corner, and return to dashboard from anywhere in the Console.
- **Help Icon:** The Help icon on top-right takes you to the **Support** page where you can opt from multiple options to contact Arcserve and view Online help for the Console.
- **Alert Icon:** The exclamation mark icon on top-right displays messages from the Console for your consideration. The messages are categorized as **Critical**, **Warning** or **Information**. You can Acknowledge the messages and take action when required. For more details, view How to Manage Alerts.
- **User Login Icon:** The icon on top-right corner displays the profile picture of the logged-in user. The icon provides option to log out from Cloud Console and update user profile of the logged-in user.

Using User Profile, you can make two updates:

- **Update Contact Information:** From **My Profile** screen, you can update your contact details and upload photo. Click **Save Changes** after making updates.
- **Change Password:** Provide a new password and click **Update Password**.
- **Two-Factor Authentication:** Provide the current password, and then do one of the following:
  - To enable two-factor authentication, click **Enable Two Factor Authentication**.
  - To disable two-factor authentication, click **Disable Two Factor Authentication**.
  - To generate two-factor codes, click **Generate Two Factor Codes**.

Monitor

After logging into Arcserve® Business Continuity Cloud, you land on the Console dashboard where Monitor displays the details of your product using multiple wizards. From the Monitor, you can perform the following options:

- **View Summary:** Monitor displays Source Summary, Usage Summary and Policy Summary for the organization.
  - **Source Summary:** Displays the count of Total Sources and the count of sources with Protected, Offline or Unprotected status based on the last backup job result.
  - **Usage Summary:** Displays the usage summary of Cloud Direct Volumes and Cloud Hybrid Stores.
  - **Policy Summary:** Displays the count of Total Policies and the count of policies with Success, Deploying, Failure or Disabled status.

    Note: Clicking on the hyperlinked status terms leads you directly to the respective detailed screen. For example, from **Source Summary**, clicking **Protected** leads you to the Sources screen that displays the list of protected sources.
- **View Details as Graphs:** For better monitoring of key details, Monitor displays graphical view of multiple fields. For example:
  - **Backup Job Summary:** Displays the last 24 hours Backup Job count for Finished, Canceled, or Failed status. Hover over the graph to view the percentage for each status.
  - **Recent 10 Jobs in Progress:** Displays recent 10 jobs in progress, supports view log or cancel job action for all *in progress* job. Clicking **View all jobs** link leads you to the Jobs screen.
  - **Top 10 Sources:** Display top 10 sources per specific condition. Supports selected Backup Job Status, Events, Job Durations, and Data Transferred.
  - **Top 10 Polices:** Displays top 10 policies and group by Job status as Finished, Failed, Canceled, or Active.
  - **Usage Trend for Cloud Direct Volumes:** Displays Usage Trend for Cloud Direct Volumes by Full backup data and group by volume name.
  - **Usage Trend for Cloud Hybrid Stores:** Displays Usage Trend for Cloud Hybrid Stores and group by Cloud Hybrid Store name.

- **Data Transfer Summary For Cloud Direct Volumes:** Displays Data Transfer Summary for Cloud Direct Volumes and group according to Data Processed, Data Transferred, or Data Written.
- **Dedupe Savings Trends For Cloud Hybrid Stores:** Displays Dedupe Savings Trends For Cloud Hybrid Stores and group by Source Data or Dedupe Savings size.

- **View Cloud Hybrid Details:** View usage trend and dedupe savings trend for Cloud Hybrid Stores. Hover over the graph to view details.
- **Expand or Collapse widgets:** Use the icon placed above a displayed widget to expand or collapse.

Protect

Using the Console, you can protect Sources, Recovered Resources, Destinations, and Policies.

What's Next!

- Protect Sources
- Protect Recovered Resources
- Protect Destinations
- Protect Policies

Protecting Source

Using the Sources option, you can add sources or protect existing sources. A node refers to a physical or agentless virtual source machine on hypervisors that you want to protect. You can protect a node by backing up data to a destination. From the Source screen, you can perform multiple options. For example:

- **Maximize of Minimize Source Screen:** Click the icon  placed on top to maximize the Source screen and to bring to default minimized size.
- **View Existing Sources:** The Source screen displays all the available sources with the details that you define in settings.
- **Define Settings:** Click the icon  to define options that you want to view for details of source. From the displayed list, select the options that you want displayed for sources.
- **Search Sources:** Provides multiple options to search added sources.
- **Save a Search:** Lets you provide a name to a search result and save with a unique name for future reference.
- **Manage Saved Search:** Lets you view all the saved searches and take collective action on any group. For more details, see How to manage saved search.
- **Actions:** From the Source screen you can perform either global or individual action on sources. For list of global and individual actions, view following links:
  - For list of global and individual actions, view following links:
    - How to Perform Common Individual and Global Actions
    - How to perform individual actions for Cloud Hybrid
    - How to perform global actions for Cloud Hybrid
    - How to perform individual actions for Cloud Direct
    - How to perform global actions for Cloud Direct
- **Download Cloud Direct Agent:** Lets you download an agent that is required to add a source.
- **Add Source:** Lets you add a new source. You must download an agent before adding a source.

View Existing Source

From the Source screen, you can view complete list of sources added before. With every source, multiple details are visible. Type, Source name and the action drop-down list at the end are default options.

For list of global and individual actions, view following links:

- How to Perform Common Individual and Global Actions
- How to perform individual actions for Cloud Hybrid
- How to perform global actions for Cloud Hybrid
- How to perform individual actions for Cloud Direct
- How to perform global actions for Cloud Direct

You can select other options to appear in the detail field according to your requirement. To customize, click the **Settings** icon  .

Some of the details displayed for source are as follows:

- **Type:** Refers to the type of source. The source is either a machine or a node on a machine.
- **Name:** Refers to the name of source. You can click the name and view details about a source. From the screen of source, you can perform multiple actions on a source. For more details, see View a Source.
- **OS:** Refers to the operating system of the source. The operating system is Windows, Linux or Mac.
- **Status:** Refers to the current status of the source. A source is either protected or not protected.
- **Connection:** Refers to the online or offline status of the source based on the connection to Internet.
- **Latest Recovery Point:** Displays the date and time of last recovery.
- **Latest Job:** Refers to the name of a job or number of jobs performed recently.
- **Policy:** Refers to the name of policy assigned to a source.
- **Source Group:** Refers to the name of group or else number of groups assigned to the source.
- **VM Name:** Refers to the name of VM for the source.
- **Agent:** Refers to the name of agent linked to source.

- **Organization:** Refers to the name of organization assigned to the source.
- **Hypervisor:** Refers to the name of Hypervisor for the source.
- **Drop-down Option for Action:** The drop-down option at the end of details for a source lets you perform multiple actions on one source. This option is applicable only to one source. View details and prerequisites for individual actions of Cloud Direct and Cloud Hybrid.

Search Source

You can search sources using multiple filters. To search, you can either enter the name directly and click the search icon or else click the drop-down arrow available in the Search box to select one or more filters and click **Search**.

Some of the available search filters for source are as follows:

- **Protection Status:** Refers to the current status of the source. A source is either protected or not protected.
- **Connection Status:** Refers to the online or offline status of the source based on the connection to Internet.
- **Job Status:** Refers to the job status of the source. The status is one of the following: In progress, Finished, Canceled, Failed, Warning, Skipped, Stopped.
- **OS:** Refers to the operating system of the **Type** of source. The operating system is Windows, Linux or Mac.
- **Source Groups:** Refers to the name of group that you can select.
- **Protection Policy:** Refers to the name of policy that you can select.

You can also save a search with results. For more details, view Save Search.

Save a Search

You have performed a search. After viewing results, you want to keep the results with search term for future reference. How can you do that?

Arcserve® Business Continuity Cloud reduces your multiple search efforts. From the Console, you can opt to save search results with a unique name. When you *perform a search*, the search results appear on the screen and the search term is displayed below the Search box at the **Search results for:** option. You can opt to either **Clear All** search terms or **Save Search**.

To save, click **Save Search**. A dialog for Save Search appears. Enter a unique name in the **Save Search Name** box and click **Save Search**. A message confirms successful action. The saved search name appears always in front of **Saved Searches**. You can click the name to view results even later without having to repeat the search.

You can later delete or update a saved search using Manage Saved Search.

Perform Global Actions on Sources

From the Source screen, you can perform multiple actions on one or multiple sources together. Simply, select the checkbox of one or more sources and click the drop-down option of Actions on top of the screen. Selected options display the number of sources that you have selected.

From the drop-down list, you can perform following actions on selected sources:

- **Start Backup:** Click to start backup for all the selected sources.
- **Cancel Backup:** Click to cancel backup for all the selected sources.
- **Assign Policy:** Click to assign same policy to all the selected sources. From the dialog of **Assign Policy**, select a policy that you want to assign and click **Confirm**.
- **Remove Policy:** Click to remove policy together from all the selected sources.
- **Delete:** Click to remove the selected sources from Console.

Apart from these collective actions, you can also perform individual actions on a specific source. For more details, see Perform Individual Actions on a Source.

For list of global and individual actions, view following links:

- How to Perform Common Individual and Global Actions
- How to perform individual actions for Cloud Hybrid
- How to perform global actions for Cloud Hybrid
- How to perform individual actions for Cloud Direct
- How to perform global actions for Cloud Direct

Perform Individual Actions on a Source

From the Source screen, you can perform individual actions on a specific source. Simply, select the drop-down arrow placed at the end of the source and select desired option from the list of displayed actions.

From the drop-down list, you can perform following actions on a source:

- **Start Backup:** Click to start backup of the source.
- **Cancel Backup:** Click to cancel backup for the source.
- **Start Recovery:** Click to start recovery of the source.
- **Assign Policy:** Click to assign a policy to the source. From the dialog of **Assign Policy**, select a policy that you want to assign and click **Confirm**.
- **Remove Policy:** Click to remove policy from the source.
- **Delete:** Click to remove the source from Console.
- **Cancel Replication(In):** Click to cancel scheduled Replication(In) for the source.
- **Deploy Policy:** Select a source and click **Deploy** from contextual actions menu to deploy policy configuration for the selected source.

  Note: The following actions do not appear for suspended organization:

  - Start Backup
  - Assign policy
  - Remove policy
  - Deploy policy
  - Cancel Replication(In)

Apart from these individual actions, you can also perform global actions together on multiple sources. For more details, see Perform Global Actions on Sources.

For list of global and individual actions, view following links:

- How to Perform Common Individual and Global Actions
- How to perform individual actions for Cloud Hybrid
- How to perform global actions for Cloud Hybrid
- How to perform individual actions for Cloud Direct
- How to perform global actions for Cloud Direct

Download Cloud Direct Agent

Important! For trial organization, the 'Download Cloud Direct Agent' button is available when trail is activated from the Monitor page or Entitlements page.

Use the option to add sources from Windows, Linux, and Mac Operating Systems. For the selected operation type, you can also select the system type between 64 bit and 32 bit. After downloading, you need to complete deployment of agent and configure for Arcserve® Business Continuity Cloud. For more information, click link.

Note: You can also download the .OVA file used for virtual Appliance, at the Download Cloud Direct Agent window.

Add a Source

Before adding a source, you must download an agent.

Follow these steps:

1. From the Source screen, click **Add a Source**.

   The Add Sources screen appears displaying the downloaded agents.

2. Select a Hypervisor.

   List of VMs available for selected Hypervisor is displayed.

3. From the list of displayed VMs, select desired VMs.

4. Click **Add Selected VMs**.

   Based on selection, sources are added as Machines or Agentless VMs.

   Warning: As each VM gets backed up in sequence, few of our customers experienced backup delays when they tried to back up more than 15 VMs from a single host. Your backup performance depends mostly on data change rate, disk performance, and network bandwidth. If you encounter such issues, please use multiple hosts. This warning is pertinent to only agentless machines running on VMware Hypervisors.

You can also view the configuration of an existing source. For more details, see View Source.

View a Source

You can view the details of an existing source from the screen of that source. To reach the screen, simply click the name of a source. The details about source is categorized into four tabs:

- **Information:** The tab provides general information and also lets you perform individual action on the source. The tab also lets you download the Agent when you click the hyperlinked name of Agent. You can also perform all the individual actions on the source using the **Actions** drop-down option. For more information, view Perform Individual actions on a source.
- **Jobs:** Provides list of jobs associated with the source. Jobs are categorized according to the following status: Jobs in Progress, Failed Jobs, Canceled Jobs, and Successful Jobs. Clicking the name of jobs takes you to the job page that displays information about the respective job. View Job description, such as Name of job, type of job, status of job, policy associated with source, destination of recovery point, duration, start and end time of job.
- **Log:** The Log tab provides complete list of logs for the source. From the **Log** tab, you can search specific logs without saving the search. You can also **Export** the log as .csv file. The log of a source provides the following information:
  - **Date:** Refers to the date when log was generated.
  - **Severity:** Refers to the information related to severity.
  - **Generated from:** Refers to the location from where the log was generated.
  - **Job Type:** Refers to the type of job performed.
  - **Message ID:** Refers to the unique ID generated for the message of log.
  - **Message:** Refers to the details provided about the specific log.
  - **Job Name:** Refers to the name of job. You can click the name of a job to view job details.
- **Recovery Points:** The Recovery Points tab displays all the recovery points linked with the source. You can search the recovery points without saving the search. The Recovery Points list displays the following information:
  - **Created on:** Refers to the date and exact time when the recovery point was created.
  - **Contents:** Refers to the location of Recovery point.

- **Policy:** Refers to the name of policy associated with the source.
- **Destination:** Refers to the destination of recovery point.
- **Drop-Down:** The drop-down arrows let you perform multiple action on a recovery point. For example, you can select to **Pin** or **Recover** a recovery point.

Protecting Recovered Resources

Using Recovered Resources feature, you can view the list of resources that you have recovered. The recovered resources are categorized according to type. For example, Recovered VMs. A key benefit of Arcserve® Business Continuity Cloud Disaster Recovery is providing customers the ability to run virtual instances of protected systems in the cloud in the event that a disaster impacts their on-premises environment. The process of powering on virtual instances of servers in the cloud and leveraging the cloud as a recovery site is often referred to a Failover.

Considerations to create Recovered Resources for a source

- If the source is a machine, assign the source a Cloud Direct Disaster Recovery as a Service Policy.
- If the source is an agentless VM, ensure that the hypervisor policy destination is a Disaster Recovery destination. As a result, all sources in the hypervisor policy are added as recovered resources.

About Failover

The Failover process involves all steps necessary to ensure that a customer can leverage the cloud as they would their on-premises environment to continue running their critical business operations. Important aspects of the Failover process include powering on virtual instances of protected systems in the cloud and enabling secure connectivity to the recovered environment.

What's next!

- Activating Arcserve Business Continuity Cloud
- Connecting to the Arcserve Business Continuity Cloud

Activating Systems in the Arcserve® Business Continuity Cloud

To activate a system in the Arcserve® Business Continuity Cloud, follow one of the methods:

- From Protect > Sources, select the source and click **Provision** from the **Actions** menu. The system starts with the latest recovery point.
- From Protect > Recovered VMs, select the recovered VM and click **Provision** from the **Actions** menu. The system starts with the latest recovery point.
- From Protect > Sources, click the source and select the option of **view details**. From the source page, click the **Recovery Points** option, select a recovery point and click **Provision** from the action drop-down option. The system starts with the latest recovery point.
- From Protect > Destinations, click the destination and select the option of **view details**. From the destination screen, click **Recovery Points** option, select a recovery point and click **Provision** from the action drop-down option. The system starts with the latest recovery point.

You have activated the system in Cloud successfully. Now, you can connect to the Arcserve® Business Continuity Cloud.

Connecting to the Cloud

You can use multiple options for securely connecting to Arcserve® Business Continuity Cloud in order to leverage the virtual instances of recovered servers.

This section contains the following topics:

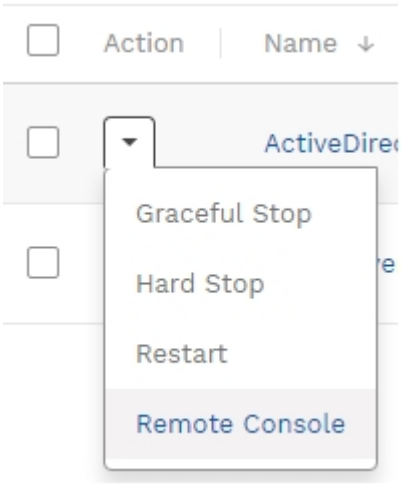
- How to Connect to Remote Console
- How to Connect to Point to Site VPN

How to Connect to Remote Console

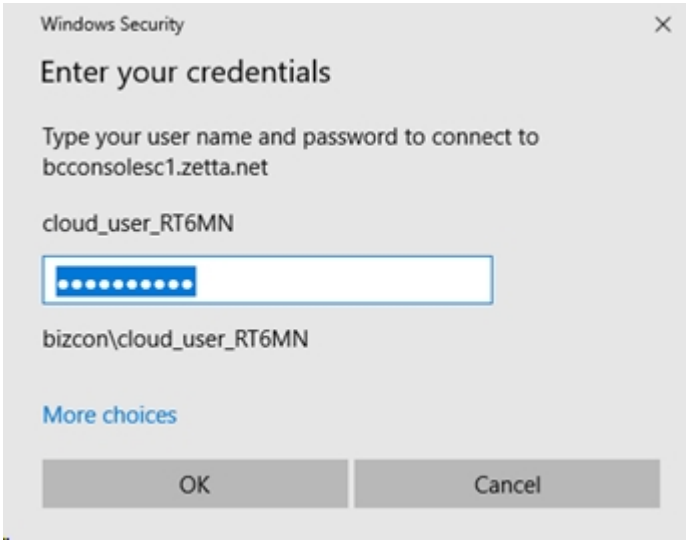
You can establish a remote console with a single virtual instance running in the Arcserve® Business Continuity Cloud. A remote console connection enables a user to access a virtual instance running in the cloud using the remote desktop protocol.

To establish a remote console connection with an activated virtual instance from the *Recovered Resources* page, follow these steps:

1. Click *Actions* > *Remote Console* for the activated system to download the remote desktop protocol (.rdp) file.



2. Launch the downloaded remote desktop protocol (.rdp) file.
3. Click *Connect* in the RemoteApp program dialog box.
4. Enter the password from the Login Credentials pop-up window into the Windows security dialog box.



5. Click *OK* to initiate the remote console connection. A web browser window should appear with the login screen of the virtual instance.
6. Click *Yes* when asked do you want to connect despite certificate errors.
7. Click Send Ctrl+Alt+Del at the top of the browser window.
8. Enter the Windows credentials for the virtual instance which are the same Windows credentials for the on-premises system at the time of the restore point.

You have connected to the remote Console successfully.

How to Connect to Point to Site VPN

A *Point to Site* connection enables a secure virtual private network (VPN) connection between a single client machine and the virtual private data center in Arcserve® Business Continuity Cloud. Such a connection would enable an end user at a coffee shop to establish a secure private connection to the recovered environment in the cloud.

Note: A separate connection is required if the end user also requires access to systems that are still available in the on-premises environment. The on-premises systems cannot communicate with the recovered systems in the cloud via the "Point to Site" connection.

To access the instructions that help to establish a *Point to Site* connection, navigate to Configure > Network Configuration, then click on **View Instructions**.

Protecting Destinations

A destination is a location where you store your backup data. A destination needs a recovery point server. Use the Destination tab to view and manage existing destinations. You can also add new destinations.

- View and Manage Destination
- Modify Destination

Add a Destination

Important! For trial organization, you can create destination after trial is activated from the Monitor page or Entitlements page.

To add a destination, you must have the data center that acts as server.

Notes:

- For Customers under MSP (sub-organizations), only MSP / MSP account admin can add a destination.
- To add Cloud Direct destination, MSP/MSP Account Admin should connect using **View as End-User Admin**.
- To add destination for Arcserve UDP Cloud Hybrid, contact Arcserve Support.

Follow these steps:

1. From the Destination screen, click **Add Cloud Volume**.

   Add Cloud Volume dialog box appears with the **Account Name** displayed.

2. Enter the following details:
   - Volume Name: Enter a unique name.
   - Data Center: Select from the available list of options.
   - Retention: Select the desired duration for retention. For more information, view how to use retention settings.

3. Click **Add Cloud Volume**.

   The destination is added and you can view or modify from the Destination screen.

View and Manage Destinations

The Destination tab lets you view and manage destinations that are already added. From the Destination screen, you can perform the following actions:

- **Search Destination:** Use the search bar to provide filter option and search destination. You can also Save Search for future usage.
- **View Details about destination:** You can specify the details to view for a destination. Using Settings icon, select the options. For example, Storage Usage, Latest Job, Location, Data Center Region.
- Manage Destination: You can Edit or delete a destination. You can also View Recovery Points assigned to a destination.
  - **Edit** Destination: From the drop-down option of a destination, click **Edit** and modify the destination.
  - **View Recovery Points**: From the drop-down option of a destination, click **View Recovery Points**. From the Recovery points tab of that destination, you can view details about recovery points.
  - **Delete:** From the drop-down option of a destination, click **Delete**. A confirmation dialog appears. Click **Confirm** to delete.

    Note: For sub-organizations, only MSP / MSP account admin can delete a destination.

For list of global and individual actions, view following links:

- How to Perform Common Individual and Global Actions
- How to perform individual actions for Cloud Hybrid
- How to perform global actions for Cloud Hybrid
- How to perform individual actions for Cloud Direct
- How to perform global actions for Cloud Direct

You can also click the name of a Destination to modify and view Capacity Usage Trend.

Modify Destination

From Destination screen, click name of a destination to modify. The selected destination opens in new screen displaying the following three tabs:

- **Information**: The tab provides General information. You can update the **Name** and click **Save Changes**. You can also view following Information:
  - **Cloud Direct:** View information about Status, Region, Volume Type, Retention period.

    Note: Retention period is divided into hourlies, weeklies, monthlies, dailies, and yearlies. For more information, view how to use retention settings.
  - **Cloud Hybrid:** View information about Status, Region, Concurrent Active Nodes Limit, Source, Dedupe Savings, Policy, Storage Usage, and Latest Job. You can also view Deduplication and Compression status.
- **Recovery Points:** Lets you search the recovery points as well as recover or pin and download files/folders. From the tab, you can view following details about the selected destination:
  - **Created On:** Refers to the date and time of creation.
  - **Source:** Refers to the name of sources assigned.
  - **Contents:** Refers to the location of data.
- **Metrics:** Lets you view **Capacity Usage Trend** of the destination. You can select the number of days to view the report. The report provides information separated into Primary and Snapshot for the Full Backup data.

Protecting Policies

A policy refers to the set of rule created to protect the data. Adding a policy requires a destination and configuring schedule to protect data.

Using the Policies feature in the Console, you can view the policies assigned to a source. From the screen, you can perform the following actions:

- **Search and Save:** You can search policies using multiple filters. To search, you can either enter policy name directly and click the search icon or else click the drop-down arrow available in the Search box to select one or more filters and click **Search**. You can also save a search with results. For more details, view Save Search.
- View Policy Details: From the policy screen, you can view list of available policies with the following details:
  - **Status:** Refers to the current status of policy such as Deploying, Disabled, Success, or Failure.
  - **Protected Sources:** Refers to the number of protected sources using the policy.
  - **Unprotected Sources:** Refers to the number of unprotected sources using the policy.
  - **Source Group:** Refers to the name or number of source groups using the policy.
  - **Latest Job:** Refers to the type of latest job with date and time. You can click the job type to view job details.
  - **Description:** Refers to the field displaying related details.
  - **Policy Type:** Refers to the field, which displays the type of policy created such as Cloud Direct BaaS, Cloud Direct DRaaS, Cloud Hybrid Replication, or Cloud Direct Agentless.
  - **Drop-Down:** Using the option, you can perform multiple actions on a policy. For example, delete or modify.
- **Modify a Policy:** To modify a policy, either use the **Modify** option available as individual action or click the name of a policy and on the policy screen to modify details of the policy. You can modify all the available policies of any protection type.
- **Delete a Policy:** Select a policy and click **Delete** from the **Actions** menu to remove a policy.

- **Deploy Policy:** Select a source and click **Deploy** from contextual actions menu to deploy policy configuration for the selected source.
- **Add a Policy:** From the policy screen, you can create new policy. You cannot add policy for Hypervisor.

  To add a policy, view the following options:

  - Add a Policy for Cloud Direct Backup
  - Add a Policy for Cloud Direct Disaster Recovery
  - Add a Policy for Cloud Hybrid Replication
- **Enable Policy:** To enable a policy, from the **Policies** screen, using the **Action** drop-down list, click **Enable**. For more information, see Enable Policy.
- **Disable Policy:** To disable a policy, from the **Policies** screen, using the **Action** drop-down list, click **Disable**. For more information, see Disable Policy.
- **Global Action:** Select multiple policies and click **Actions** drop-down arrow from the top. From the displayed options, you can perform multiple actions on selected policies. For example, click **Delete** to remove all the policies.
- **Individual Action:** Click the drop-down arrow for a policy and from the displayed options, you can perform multiple actions on selected policy. For example, click **Delete** to remove a policy or click **Edit** to modify the details of existing policy.

  For list of global and individual actions, view following links:

  - How to Perform Common Individual and Global Actions
  - How to perform individual actions for Cloud Hybrid
  - How to perform global actions for Cloud Hybrid
  - How to perform individual actions for Cloud Direct
  - How to perform global actions for Cloud Direct

Add a Policy for Cloud Direct Backup

Important! The first policy is added by default on Enrollment for Direct Backup. Later, you can modify the policy or add new policies.

Notes:

- For trial organization, the default policy and destination are available when the trial is activated from the Monitor page or Entitlements page.
- If the organization gets suspended, **Add a Policy for Cloud Direct Backup** does not work.

Adding a policy for Cloud Direct Backup involves multiple steps.

Follow these steps:

1. From the Policy screen, click **Add Policy**.

   The Add policy screen appears with three tabs.

2. Click the first tab - **Basics** and perform the following steps:
   - Enter a **Policy Name**.
   - Select Cloud Direct Backup as the **Protection Type** .
   - Enter description if desired.
3. If you want to assign sources, click the second tab - **Source (Optional)** and perform the following steps:
   - You can use the **Search** box to find a matching source from the sources already added or else directly click **Select Source(s)** to view available sources.
   - From the displayed list of sources, select checkbox of one or more sources to add to the policy.

     Note: Add sources of the same operating system. For example, all Windows or Mac or Linux.
   - Click **Add Source(s)**.

   The screen displays added sources.
4. Click the third tab - **Destination** where you need to define the policy in detail.

   Provide the Activity Type, location to store, and schedule to protect. Perform the following steps in the three tabs:

Note: When the Activity Type selected is Cloud Direct file folder, the **Additional Settings** tab is also displayed. The Exclude configuration is available in the Additional Settings.

- From the tab, **What to protect**, select the desired activity for the policy.

  For **File Folder**, enter a UNC or local drive path for Windows or Linux path for (Mac/Linux). If a UNC path is entered, modify the run as user of the Cloud Direct Agent option to a user with full control on the UNC path and Builtin\Administrator permissions using either of the following options:

  - Start a backup and wait until the Cloud Direct Agent attempts to mount the UNC path. On the credentials prompt, the credentials that you enter is saved for future backups.
  - Right click the Cloud Direct Agent system tray icon and click **Local Settings**. Click **Browse** to find the desired user and then enter the password.

  For **Windows image**, you can opt either for Full System or specify one or more drives. A source configured with full system updates the list of drives that is backed up every time when the Cloud Direct Agent service starts.

  For **SQL Server**, select any one of the following:

  - **Sync direct from database:** Utilizes the SQL backup providers to stream the SQL database files and log files to the cloud without writing them to locally staged space.
  - **Sync via locally staged backup:** Verify if the staging directory is on a drive with free space greater than the total size of all the databases of all the instances that you are backing up. Verify if the selected user (with the option, run as user of the Cloud Direct Agent) has sysadmin privileges on the instances that you are backing up. By default the run as user of the Cloud Direct Agent is the NT Authority\SYSTEM user.

  For **Exchange**, you can backup the Microsoft Exchange Server database.

  Note: If multiple activity types are listed in What to Protect, you can configure each unique activity type by clicking the **Add Destination** button.

- From the tab, **Where to protect**, select a destination to protect the source. If you need to **Create a local backup**, enter a local path as the Destination that is not already getting backed up in the task configuration.

  Key Considerations:

  - If the sources in the policy are Windows System, then you can enter a UNC path or local drive path. If you select the Windows Image Backup>Full System task, use a UNC path to avoid performing a local backup to a drive backing up to the cloud as the Full System task backs up all drives.
  - If the sources are Linux or Mac systems, enter a Linux path.
  - If the tasks are non-File Folder tasks, then verify if you have 2.1 times the free space on the local copy destination as the Agent creates the new local copy first, then removes the old local copy. For File Folder tasks, the recommended free space is 1.1 times the size of the source path.
  - If a UNC path is entered, modify the run as user of the CD Agent to a user with full control on the UNC path and Built-in\Administrator permissions on the source system. To modify the run as user, right click on the Cloud Direct Agent system tray icon and click Local Settings. Then, click Browse to find the user and enter the password. Start a backup and wait until the Cloud Direct Agent attempts to mount the UNC path. On the credentials prompt, the credentials that you enter is saved for future backups.
  - Do not make a local copy to a sub-path of a path or drive that you are backing up to avoid duplicate data.

- The **When to protect** tab allows you to set a schedule for backup. Multiple backup schedules are available for BaaS policies such as Every 15 Minutes, Every 1 Hour, Every 6 Hours, and Every 1 Day with a Start Time. In addition, you can add a **Throttle Schedule**.

  Note: To enable multiple backup schedules for CD BaaS policies, contact **Arcserve Support**.

- From the **Additional Settings** tab, do the following:

  - For **Cache Location**, enter the location where the cache is stored. The Cache Location locally stores cache to optimize

transfer performance. It roughly totals 1% of the data set. If free disk space is a concern, provide an alternate location for the cache.

- For **Pre-backup Script**, enter the location of the script that executes before the backup job runs.
- (Optional) To stop the backup when script fails, check the **Stop backup if the script fails** checkbox.
- For **Post-backup Script**, enter the location of the script that executes after the backup is completed.

The Create Policy button is enabled.

Note: You can also remove a destination from the policy using **Remove Destination**.

5. Click **Create Policy**.

   The added policy is displayed on the Policies screen with the current status displayed as Deploying. After completion of deployment, the status changes either to Success or Failure.

Add a Policy for Cloud Direct Disaster Recovery

Prerequisites

- A license for Disaster Recovery.
- A DRaaS (zero copy) volume

Note: If the organization gets suspended, **Add a Policy for Cloud Direct Disaster Recovery** does not work.

Adding a policy for Arcserve® Business Continuity Cloud involves multiple steps.

Follow these steps:

1. From the Policy screen, click **Add Policy**.

   The Add policy screen appears with three tabs.

2. Click the first tab - **Basics** and perform the following steps:
   - Enter a **Policy Name**.
   - Select a Cloud Direct Disaster Recovery as the **Protection Type**.
   - Enter description if desired.
3. If you want to assign source, click the second tab - **Source (Optional)** and perform the following steps:
   - Click **Select Source(s)** to view available sources.
   - From the displayed list of sources, select checkbox of one or more sources to add to the policy.
   - Click **Add Source(s)**.

   The screen displays added sources.
4. Click the third tab - **Destination** where you need to define the policy in detail.

   Provide the Activity type, location to store, and schedule to protect. Perform the following steps in the three tabs:
   - From the tab, **What to protect**, select desired activity for the policy.

     For Windows image, you can opt either for Full System or individual drives. A source configured with full system updates the list of drives that are backed up every time when the Cloud Direct Agent service starts. If you select individual drives, make sure to include your boot drive.

- From the tab, **Where to protect**, select a disaster recovery destination to protect the source. If you need to **Create a local backup**, view the following considerations:
  - If you select the Windows Image Backup>Full System task, use a UNC path to avoid performing a local backup to a drive backing up to the cloud as the Full System task backs up all drives on each source in the policy.
  - If a UNC path is entered, modify the run as user of the Cloud Direct Agent option to a user with full control on the UNC path and Builtin\Administrator permissions on the source system. To modify the run as user, right click the Cloud Direct Agent system tray icon and click Local Settings. Click Browse to find the desired user and then enter the password. Another option is to start a backup and wait until the Cloud Direct Agent attempts to mount the UNC path. On the credentials prompt, the credentials that you enter is saved for future backups.
  - Verify if you have 2.1 times the free space on the local copy destination as the Agent creates the new local copy first, then removes the old local copy.
- From the tab, **When to protect**, set a schedule for backup. Multiple backup schedules are available for disaster recovery. For example, Every 15 Minutes, Every 1 Hour, Every 6 Hours, Every 1 Day with a Start Time. You can also opt to add a **Throttle Schedule**.

Create Policy button is enabled.

5. Click **Create Policy**.

   The added policy is displayed on the Policies screen with the current status displayed as Deploying. After completion of deployment, the status changes either to Success or Failure.

   After a successful deployment, a Recovered Resource is created for the source and visible at the Recovered Resources tab.

Add a Policy for Cloud Hybrid Replication

Note: If the organization gets suspended, **Add a Policy for Cloud Hybrid Replication** does not work.

Adding a policy for Arcserve® Business Continuity Cloud involves multiple steps.

Follow these steps:

1. From the Policy screen, click **Add Policy**.

   The Add policy screen appears with three tabs.

2. Click the first tab - **Basics** and perform the following steps:

   - Enter a **Policy Name**.
   - Select Cloud Hybrid Replication as the **Protection Type**.
   - Enter description if desired.

   The Source tab is disabled.

   Now, you can add two tasks to the policy.

3. Click the third tab - **Destination** where you need to define the policy in detail.

   Provide the Activity type, location to store, and schedule to protect. Perform the following steps in the three tabs:

   - In the tab, **What to protect**, select desired activity for the policy.

     Replicate from a remotely-managed RPS. To configure this activity refer to **Replicate from a remotely-managed RPS** task in *Arcserve UDP Solutions Guide*.

   - In the tab, **Where to protect**, select a destination to protect the source.
   - In the tab, **When to protect**, set a Merge schedule.
   - In the tab, **Additional Settings**, you can also opt to add Retention Policy to retain **Daily Backups**, **Monthly Backups**, **Weekly Backups**, and **Manual Backup**.

   Note: You can also remove a destination from the policy using **Remove Destination**. But if you configured with the Replicate to a remotely-managed RPS task, you need to remove that first before removing the Replicate from a remotely-managed RPS task.

4. (Optional) From the third tab - **Destination**, add a new task **Replicate to a remotely-managed RPS** for reverse replication. To configure this activity refer to **Replicate to a remotely-managed RPS** task in *Arcserve UDP Solutions Guide*. Perform the following steps:

   - Click the cross icon to close the Replicate from a remotely-managed RPS task.
   - Click the Hyperlink icon to add a Replicate to a remotely-managed RPS task.
   - Click the Replicate to a remotely-managed RPS task.
   - In the **Where to protect** tab, provide remote UDP Console access information to get share plan.
   - In the **When to protect** tab, add Replicate Schedule and Throttle Schedule.

   Note: You can also remove a destination from the policy using **Remove Destination**.

   The Create Policy button is enabled.

5. Click **Create Policy**.

   The added policy is displayed on the Policies screen with the current status displayed as Success, Fail or Deploying. You can also modify the policy later. Click the policy name from the Policy screen and make updates.

   Note: You can protect Agent-based, OneDrive, CIFS, Agentless nodes of Arcserve UDP in Arcserve Cloud by configuring Cloud Hybrid Replication task. For more information, refer to Configure Replicate to Arcserve Cloud task.

Modify a Hypervisor Policy

You can modify policies for all protection types. Here is an example of how to modify policy of hyperfvisor.

Follow these steps:

1. From the Policy screen, click **Add Policy**.

   The Add policy screen appears with three tabs.

2. Click the first tab - **Basics** and perform the following steps:

   - Enter a **Policy Name**.
   - Select a **Protection Type**. For example, Cloud Direct Backup or Cloud Hybrid Replication.
   - Enter description if desired.

3. If you want to assign source, click the second tab - **Source (Optional)** and perform the following steps:

   - You can use the **Search** box or else directly click **Select Source(s)** to view available sources.
   - From the displayed list of sources, select checkbox of one or more sources to add to the policy.
   - Click **Add Source(s)**.

   The screen displays added sources.

4. Click the third tab - **Destination** where you need to define the policy in detail.

   Provide the source, location, and schedule to protect. Perform the following steps in the three tabs:

   - In the tab, **What to protect**, select desired activity for the policy.

     For Windows image, you can opt either for Full System or specify one or more drives

   - In the tab, **Where to protect**, select a destination to protect the source. If you need to **Create a local backup**, enter a local path as the Destination.
   - In the tab, **When to protect**, set a schedule for backup. You can also opt to add a **Throttle Schedule**.

   Create Policy button is enabled.

5. Click **Create Policy**.

   The added policy is displayed on the Policies screen with the current status displayed as Deploying. After completion of deployment, the status changes either to Success or Failure.

Analyze

The Analyze feature lets you view Jobs, Log, and Reports. The icon on top lets you collapse or expand the screen.

What's Next!

- Analyze Jobs
- Analyze Logs
- Analyze Reports

Analyzing Jobs

Displays complete list of jobs with the details that you can customize.

Key Highlights

- The search bar helps you find a job according to the selected filters. For example, status, job type, date range or protection policy.
- You can save the search also for future usage.
- Manage Saved Search option lets you manage a search if you have saved. For more information, view how to manage saved search.
- All the jobs display details that you can customize by using the Settings icon. Jobs are divided into multiple categories based on status. For example, Jobs in Progress, Failed Jobs, Canceled Jobs, and Successful Jobs.
- View Job description, such as Name of job, type of job, status of job, policy associated with source, destination of recovery point, duration, start and end time of job. You can also view the job description from the Jobs tab on the screen of a source.
- For every job, you can **view log**. Click the drop-down option placed at the end of every row of a job to view log of that job.
- You can also **Cancel** a job that is in progress.

  For list of global and individual actions, view following links:

  - How to Perform Common Individual and Global Actions
  - How to perform individual actions for Cloud Hybrid
  - How to perform global actions for Cloud Hybrid
  - How to perform individual actions for Cloud Direct
  - How to perform global actions for Cloud Direct

Analyzing Logs

The log tab displays all activity logs for the protected nodes, destination servers, data stores, and policies. You can view logs and apply various filters such as severity, logs generated from the machine, job type, and log content. You can also Export logs. Message ID provides a hyperlink to access detailed documentation. Click the hyperlink in the MessageID column to view the description and solution for that message. On the log screen, Message IDs are displayed only for Replication IN jobs.

Export Logs: From the Log screen, you can export the logs to your Inbox. Click **Export** from the top of Log screen and the log is sent to your registered email ID. In your inbox, find the email from Arcserve Cloud Support email with the subject Log Export and click **Download Export** in the email to download log as .csv file.

Search Logs: You can search the activity logs using a combination of the available filters or one of the following options and clicking **Search**:

- Select **Severity** types to view all the logs related to the selected type.
- Select **Job Type**.
- Select **Date Range**.
- Select **Generated From** location.
- Enter message term in the Search box.

Analyzing Alert Reports

Use Arcserve® Business Continuity Cloud to analyze alerts separately or together based on the alert type.

From the list of alerts, you can view alert details such as Alert Name, Alert Type, Report for, Created on, Last Generated, and Recipients.

From the Alerts screen, you can perform following actions:

- Create a New Alert Report
- Edit an Alert Report

Create a New Alert Report

Using **Create Alert**, you can add new alert report. The alert report is sent as a link to the email and additional recipients, if added. The **Create Alert** report wizard is required to create new report. The wizard appears when you click **Create Alert** on the alerts page.

Follow these Steps:

1. From the Analyze screen, click **Alerts** tab.

   The Alerts screen appears.

2. From the Alerts screen, click **Create Alert**.

   The Create Alert wizard appears.

3. From the **Create Alert** wizard, from **Alert Type**, select one of the options.
4. For Alert Name, enter a unique name for your new alert report.
5. Select one of the following options:
   - **Report all Sources:** Lets you generate report from all available sources.
   - **Report selected Source Groups:** Lets you generate report only from the selected source groups. If you select this option, from the drop-down option, select Source Groups, and then click **Add**. To select multiple groups, repeat the action.
6. (Optional) To share your report with others, enter email addresses of one or more recipients, and then click **Add**.
7. Click **Create**.

   A confirmation dialog appears that displays the successful generation of the alert report.

The Alert Report screen contains the success report. When the backup is completed, an email is sent to the logged in user and other recipients, if any.

Edit an Alert Report

You can edit an Alert Report in the Alerts page.

Follow these steps:

1. From the Analyze screen, click **Alerts**.

   The Alerts – Reports screen displays a List of reports. From the list, click the name of an Alert Report or use the drop-down option to select the report, and then click **Edit**.

   The Edit Report Settings screen appears.

2. From the screen, select one of the options to specify the sources:
   - **Report all Sources:** Lets you edit reports from all available sources.
   - **Report selected Source Groups:** Lets you edit reports only from the selected source groups. If you select this option, from the drop-down option, select Source Groups, and then click Add. To select multiple groups, repeat the action.
3. To share your report with others, enter email addresses of one or more recipients, and then click **Add**.
4. Click **Save Changes**.

   The report is modified.

Analyzing Reports

Arcserve® Business Continuity Cloud helps you analyze the report together as well as separately according to the report types. From the Report screen, you can search for reports using the filters of Date Range, Schedule for, and Generate on. Also, you can save the search item.

From the list of reports, you can view details about a report. For example, Report Name, Date Range, Report for, Generated on, Scheduled for, Report type, Created by, and Recipients. From the report screen and related screens, you can also perform following actions:

- Create Report
- View Reports
- Manage Report Schedules
- Export report
- Edit a report schedule

How to View a Report

You can manage schedules of all the report using Manage Report Schedules. Under Analyze>Reports, click Manage Report Schedules and you can view list of all reports. From the screen, you can perform the following actions:

- **Search:** To search reports, either provide a report name in the search bar or use filters of **Scheduled for** and **Report Type**.
- **View details:** The list of report provides complete details about every report. For example, Report Name, Report Type, Report for, Scheduled For, Created by, Created on, Last Generated. You can click a Report Name to edit settings of the report.
- **Global Actions:** When you select check box of one or more report names, in the top bar **Selected** shows the number of check boxes selected and **Actions** option is enabled to help you perform collective action on selected reports. For example, **Delete** all selected reports or use **Generate Now** to prepare a copy of all selected reports.
- **Individual Actions:** On a specific report, you can perform the following individual actions:
  - **Edit Report:** From the drop-down option placed at the end of a report, when you click **Edit**, the dialog **for Edit Report Settings** appears. Make required modifications and click **Save Changes**. For more details, view how to edit a report schedule.
  - **Generate Now:** From the drop-down option placed at the end of a report, when you click **Generate Now**, an instance of that report is created and appears immediately in the list of reports.
  - **Delete A Report:** From the drop-down option placed at the end of a report, when you click **Delete Report**, a confirmation dialog appears. Click **Confirm** to delete the report.

    Note: While deleting report as individual or global action, you can also delete all report instances created by a report schedule. From the confirmation message, select the check box of **delete the report instances** also.

To view details of specific reports, click on one of the following report types:

- Backup Jobs
- Policy Tasks

- Recovery Jobs
- Data Transfer
- Capacity usage

Report for Backup Jobs

From the console, click Backup Jobs below Reports to reach the screen that lets you view summary of all the backup jobs. You can also search the source using the filters of Date Range, Protection Policy, Destination or Source Groups. Using multiple filters is allowed. Click icon of Manage Saved Searches to select the option that you want to view in report.

Key Highlights:

- From the screen, you can Create Report and Export Report as .csv file.
- Hover over the chart to view percentage of Failed, Finished, and Canceled jobs.
- View top 10 sources and filter according to Backup Job Status, Events, Jobs Duration or Data Transferred.
- Hover over the graph to view classification of Finished, Failed and Canceled jobs.
- View **Details** of all backup jobs from the table.

Report for Policy Tasks

To view the policy tasks details of completed backup jobs, go to **Analyze** > **Policy Tasks**.

Click **Policy Tasks** to view the summary of the policy tasks of completed backup jobs. You can search the source using multiple filters such as Date Range, Protection Policy, Destination, and Sources Groups. On the top-right corner of the **Policy Tasks** page, click **Manage Saved Searches** and select an option that you want to view in the report.

Key Highlights

- From the screen, to create and export report as a .csv file, click **Create Report** and **Export Report** respectively.
- Hover over the chart to view the percentage of Finished, Failed, and Canceled jobs.
- Apply filters to view Top 10 Sources such as Events and Job Duration.
- Hover over the graph to view classification of Finished, Failed, and Canceled jobs.
- From the table, view Details of all policy tasks for completed backup jobs.

Report for Recovery Jobs

From the Console, click Recovery Jobs below Reports to reach the screen that lets you view summary of all the jobs recovered. You can also search the source using the filters of Date Range, Destination or Source Groups. Click icon of Settings to select the option that you want to view in report.

Key Highlights:

- Hover over the chart to view percentage of Failed, Canceled, and Finished jobs.
- View top 10 sources and filter according to Recovery Job Status, Events, Jobs Duration or Data Transferred.
- Hover over the graph to view classification of Finished, Failed, and Canceled jobs.
- View **Details** of all restore jobs from the table.
- Export the reports as CSV file.
- Create reports for individual reports for all roles.
- Manage saved search. For more information, view how to manage saved search.

Report for Data Transfer

From the console, click Data Transfer below Reports to reach the screen that lets you view summary of data transfer. You can also search the source using the filters of Date Range and Source Groups.

Key Highlights:

- Hover over the chart to view data processed, data transferred and data written on a specific date.
- Hover over the graph to view classification of Finished, Failed and Canceled jobs.
- View **Details** of all data transfer from the table.
- Export the reports as CSV file.
- Create reports for individual reports for all roles.
- Manage saved search. For more information, view how to manage saved search.

Report for Capacity Usage

From the console, click Capacity Usage below Reports to reach the screen that lets you view usage trends and dedupe savings trend. You can also search the destination using the filters of Date Range, and Destination.

Key Highlights:

- Hover over the chart to view usage trend and dedupe saving trend on different dates.
- View **Details** of capacity usage from the table.
- View details about all available destinations.
- Export the reports as CSV file.
- Create reports for individual reports for all roles.
- Manage saved search. For more information, view how to manage saved search.

Manage Report Schedules

You can manage schedules of all the report using Manage Report Schedules. Under Analyze>Reports, click Manage Report Schedules and you can view list of all reports. From the screen, you can perform the following actions:

- **Search:** To search reports, either provide a report name in the search bar or use filters of **Scheduled for** and **Report Type**.
- **View details:** The list of report provides complete details about every report. For example, Report Name, Report Type, Report for, Scheduled For, Created by, Created on, Last Generated. You can click a Report Name to edit settings of the report.
- **Global Actions:** When you select check box of one or more report names, in the top bar **Selected** shows the number of check boxes selected and **Actions** option is enabled to help you perform collective action on selected reports. For example, **Delete** all selected reports or use **Generate Now** to prepare a copy of all selected reports.
- **Individual Actions:** On a specific report, you can perform the following individual actions:
  - **Edit Report:** From the drop-down option placed at the end of a report, when you click **Edit**, the dialog **for Edit Report Settings** appears. Make required modifications and click **Save Changes**. For more details, view how to edit a report schedule.
  - **Generate Now:** From the drop-down option placed at the end of a report, when you click **Generate Now**, an instance of that report is created and appears immediately in the list of reports.
  - **Delete A Report:** From the drop-down option placed at the end of a report, when you click **Delete Report**, a confirmation dialog appears. Click **Confirm** to delete the report.

    Note: While deleting report as individual or global action, you can also delete all report instances created by a report schedule. From the confirmation message, select the check box of **delete the report instances** also.

Configure

Arcserve® Business Continuity Cloud helps you configure multiple options to have better control. For example, you can configure infrastructure, source groups, access control, licensing & subscription.

Whats Next!

- Configuring Infrastructure
- Configuring Source Groups
- Configuring Access Control

Configuring Infrastructure

Using Infrastructure feature, you can add Hypervisors to Arcserve® Business Continuity Cloud. The screen displays list of Hypervisors added for your organization. To add a hypervisor, you need to perform the following steps:

1. Set up UDP Cloud Direct Virtual Appliance
2. Configure UDP Cloud Direct Virtual Appliance
3. Delete UDP Cloud Direct Virtual Appliance

How to Set up UDP Cloud Direct Virtual Appliance

For VMware virtual environments, deploy the UDP Cloud Direct Virtual Appliance to enable agentless protection of one or more VMware virtual machines. The virtual appliance eliminates the need to install the UDP Cloud Direct agent on each virtual machine.

This section contains the following topics:

Downloading UDP Cloud Direct Virtual Appliance

The UDP Cloud Direct Virtual Appliance is available as *.ova* file at the Arcserve® Business Continuity Cloud Console. From the Console, click **Download Appliance for VMware (.OVA)** from Configure > Infrastructure > Hypervisors to download the file.

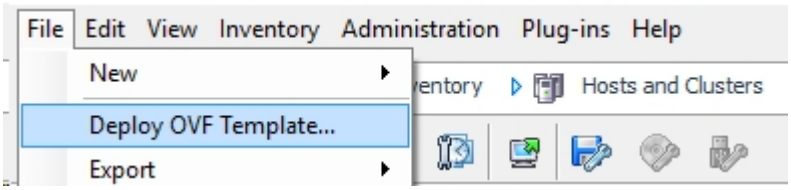
Now, you need to deploy the appliance.

Deploying UDP Cloud Direct Virtual Appliance

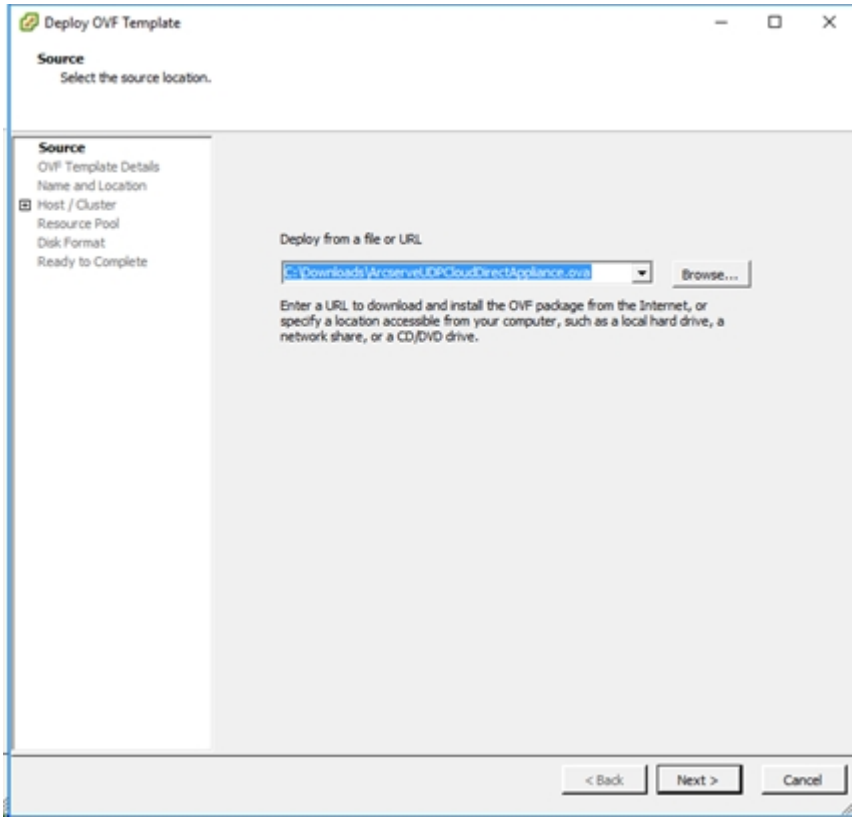
Use the VMware vSphere Web Client to deploy the UDP Cloud Direct Virtual Appliance into your VMware vSphere environment.

Follow these steps:

1. Launch the VMware vSphere Web Client and log in.
2. In the vSphere Web Client, click on File, and then select Deploy OVF Template.



3. Click ***Browse*** to select the file from the location where you downloaded the *.ova* file and click **Next >**.



4. Proceed through the rest of the setup process until you reach *Ready to Complete*, and then click **Finish**.

   The UDP Cloud Direct Virtual Appliance is deployed.

5. Once completed, click **Close**.
6. Navigate to *Getting Started* and select the UDP Cloud Direct Virtual Appliance, and then click *Power on the virtual machine*.

You have deployed the UDP Cloud Direct Virtual Appliance successfully.

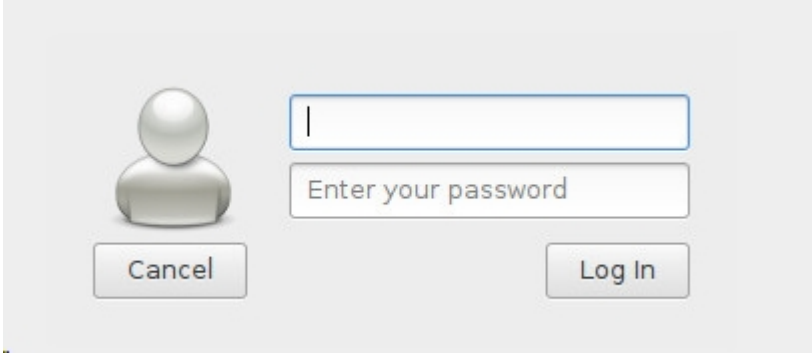
Now, you need to register the appliance.

Registering UDP Cloud Direct Virtual Appliance

Once the Virtual Appliance is installed and powered on, you need to register the UDP Cloud Direct Virtual Appliance with the Arcserve® Business Continuity Cloud.

Follow these steps:

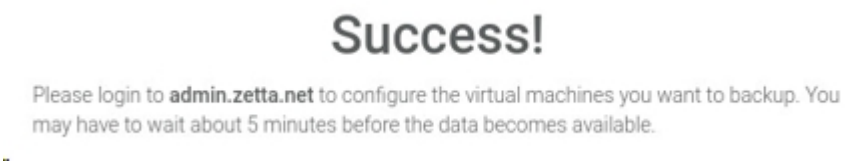
1. In the VMware vSphere Web Client, navigate to the *Console* tab for the virtual appliance.



2. Enter the default user name *zetta*, the default password *zettazetta*, and click **Log In**.
3. Enter the user account credentials (email/password) of a user created under your account that leverages the virtual appliance, and then click **Continue to vCenter Configuration**.

4. Enter your vCenter Server address, vCenter Username, and vCenter Password, and then click **Complete Configuration**.

You should get confirmation about successful completion of registration. Also, within 5 minutes data becomes available in the UDP Cloud Direct Portal.



5. **Optional step:** You can click *Change Appliance Password* to change the password for your UDP Cloud Direct Virtual Appliance using your current default password.

You have registered the UDP Cloud Direct Virtual Appliance successfully. A policy is created for the Appliance, the policy name is *<System Name> + Policy*. Now, to complete configure the appliance.

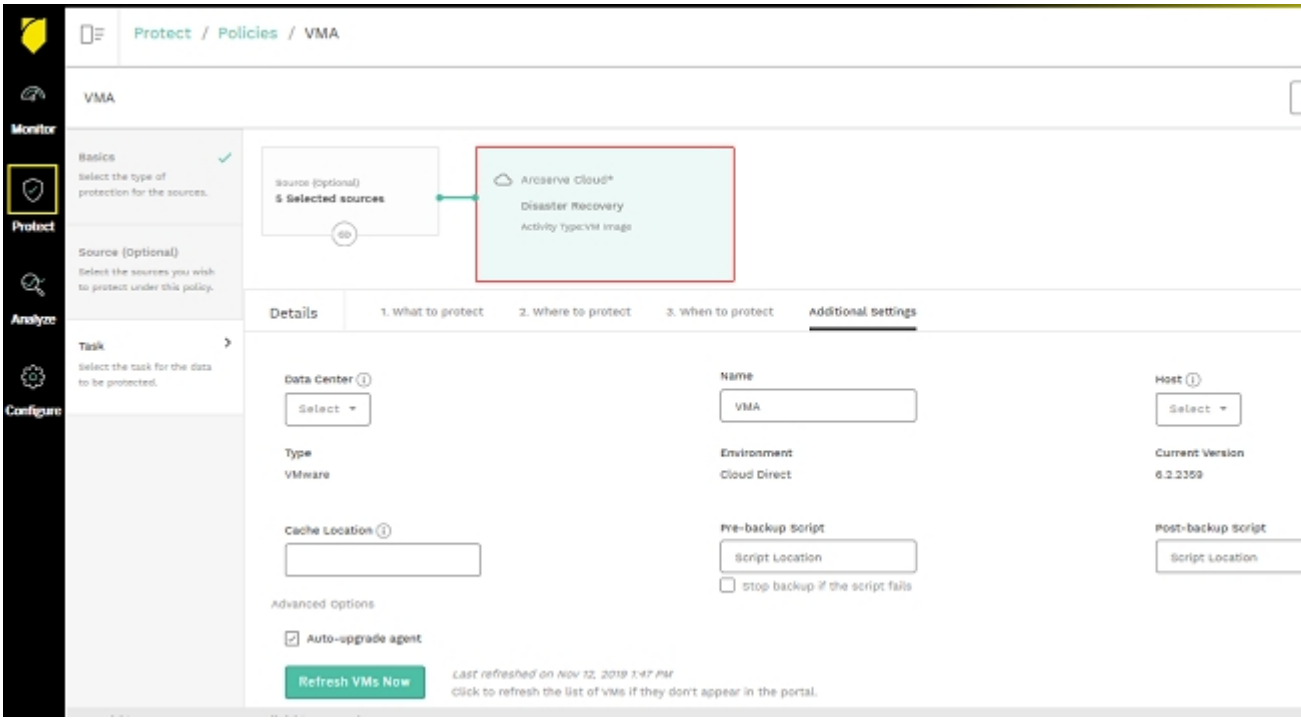
Configure UDP Cloud Direct Virtual Appliance

You can configure a virtual appliance after completion of registration to the Console. To configure, you must add the virtual machines as a source. For more information, see Add a source. Then, you can configure the settings as required.

Follow these steps:

1. From the displayed list at Configure > Infrastructure > Hypervisors, click name of the desired Virtual Appliance or from Protect > Policies, modify the Appliance policy.

   The virtual appliance policy modification page is displayed.



2. Click the **Destination** tab and perform the following steps:

   a. From the **Where to protect**, specify the desired destination where you want to store the data.

   b. From the **When to protect** tab, assign a backup schedule to run.

   Note: You can also add a Throttle Schedule to restrict bandwidth usage.

   If you select a Disaster Recovery destination, recovered resources are created for all added sources in the policy.

3. From the **Additional Settings**" tab, you can add/update the information of the following fields and click **Save**:

Data Center / Host

Default set to None. When a value is set, only virtual machines from this Data Center / Host is protected.

Note: Verify that VMs outside are already disabled.

Name

Refers to the System name provided during registration. You can modify if required.

Cache Location

Enter the location where the cache is stored. The Cache Location locally stores cache to optimize transfer performance. It roughly totals 1% of the data set. If free disk space is a concern, provide an alternate location for the cache.

Pre-backup Script

Enter the location of the script that executes before the backup job runs and to stop the backup when script fails, check the Stop backup if the script fails (Optional) checkbox

Post-backup Script

Enter the location of the script that executes after the backup is completed.

Auto-upgrade agent

Refers to the agent. Enabled by default, lets you automatically upgrade the agent in Virtual Appliance.

Auto-sync new VMs

Lets you sync the VMs from vCenter daily. The option is disabled by default. To manually sync the VMs, you can click **Refresh VMs now**.

The configuration of virtual appliance is complete.

Delete UDP Cloud Direct Virtual Appliance

You can delete an existing UDP Cloud Direct virtual appliance.

Considerations:

- If a recovered resource is running for an enabled virtual machine, you cannot delete the virtual appliance.
- All the enabled virtual machines are also deleted.

Follow these steps:

1. Navigate to Configure > Infrastructure > Hypervisors.

   All the added virtual appliances are displayed.
2. From the displayed list, click **Action** drop-down option for the desired virtual appliance.

   The option to delete appear.
3. Click **Delete**.

   A confirmation message appears.
4. Click **Yes** to confirm.

   The virtual appliance is deleted.

Set up UDP Cloud Direct Agent for Hyper-V

Perform a Hyper-V integration to protect data that resides on VMs of Hyper-V.

Follow these steps:

1. Navigate to the **Protect** screen and click **Download Cloud Direct Agent**.
2. Copy the downloaded file and paste the file to the Hyper-V machine.
3. Run the file as per the set-up instructions to complete the installation of Cloud Direct Agent.
4. After installing Cloud Direct Agent, provide your cloud account details in the registration window, to add Hyper-V to cloud console.

   The Hyper-V appears in the **Machines** field of the **Protect** Screen. The **Backup VMs** options may appear after sometime.
5. Scroll towards the far right of the source node and select **Backup VMs** option from the contextual view.

The Hyper-V gets highlighted in red in the source list and appears in the **Hypervisors** field of the **Configure** screen. The Hyper-V may appear in the **Hypervisors** field after sometime.

Subsequently, a default policy gets created in the **Polices** field of the **Protect** screen.

6. Add VMs to the Hyper-V by following one of the below methods:

   Using the Configuration Screen

   1. Navigate to the **Hypervisors** field and select a Hyper-V name to proceed to the Edit Policy page.
   2. Click the **Sources** field and click **Select Sources** to view the VMs residing on the Hyper-V.
   3. Select the checkboxes with the VM names which you want to backup and click Add Sources.

   Using the Protect Screen

   1. Navigate to the **Policies** field and select a policy that has the Hyper-V name.
   2. Click the **Sources** field and then click **Select Sources** to view the VMs residing on the Hyper-V.
   3. Select the checkboxes with the VM names which you want to backup and click Add Sources.
   4. Click the **Destinations** field and then click the Activity Type: VM Image box and edit the following fields as per your requirement:
      - Where to protect
      - When to protect
      - Additional settings
   5. From the **Additional Settings** tab, do the following:
      - For **Cache Location**, enter the location where the cache is stored. The Cache Location locally stores cache to optimize transfer performance. It roughly totals 1% of the data set. If free disk space is a concern, provide an alternate location for the cache.
      - For **Pre-backup Script**, enter the location of the script that executes before the backup job runs.
      - (Optional) To stop the backup when script fails, check the **Stop backup if the script fails** checkbox.

- For **Post-backup Script**, enter the location of the script that executes after the backup is completed.

Note: After an Agentless backup is performed, the operating system information does not appear. To display the operating system information, install the Integration Services in the guest OS and power-on the VM.

7. (Optional) If a new VM is added under Hyper-V, click **Refresh VMs Now** while modifying the policy to make them available in cloud console. Follow step 6 to manually add the VMs to Cloud Console.

   Hyper-V integration to protect data that resides on VMs of Hyper-V is now complete.

Configuring Source Group

Source Groups refer to the groups that contain multiple sources. Using the feature, you can maintain groups of specific type of sources. The Source Group screen displays the existing groups and provides option to create or delete a group. You can also use the search option to find a group.

Key Highlights:

- Search a group: From the Source Group screen, you can search a group using the **Search** option.
- View source group details: View details related to a source group. For example, Name of group, Total Assigned Sources, Protected Sources and Not Protected Sources.
- Delete a source group: Use the drop-down option available for every source group to delete a group.

For list of global and individual actions, view following links:

- How to Perform Common Individual and Global Actions
- How to perform individual actions for Cloud Hybrid
- How to perform global actions for Cloud Hybrid
- How to perform individual actions for Cloud Direct
- How to perform global actions for Cloud Direct

What's Next!

- Create a Source Group
- Assign Sources to a Source Group

Create a New Source Group

From the Source Group feature, you can create multiple groups for sources.

Follow these steps:

1. From the Source Group screen, click **Create Group**.

   Create Group dialog is displayed.
2. Enter a unique name as the **Group Name**.
3. Click **Create**.

   The new source group is visible on the Source Groups screen.

Assign Sources to a Source Group

You can assign available sources to the source groups. Simply, open a source group and assign relevant sources.

Follow these steps:

1. From the Source Group screen, click name of a source group.

   The screen of that source group displays related details.

2. Click **Add Sources to Group**.

   Add Sources to Group screen appears displaying the list of available sources

3. Select the checkbox of sources to add.

   Selected field on top shows the number of sources you opted to add.

4. Click **Add Selected Sources**.

   The source group name screen displays the number of added selected sources.

From Actions drop-down list, you can select to remove some sources from the source group. To remove one or more sources, follow these steps:

1. Select the checkbox of desired sources.
2. Click **Remove from Group** option available in **Actions** drop-down list.

   A confirmation dialog appears.

3. Click **Confirm** to remove.

Configuring Access Control

The feature lets you manage users. You can add a new user and also perform specific action for existing users.

Note: Using this option, you cannot manage your own details. You can only manage the users that you add. To reset your password, navigate to User Profile.

What's next!

- Manage User Accounts
- Manage Roles

Manage User Accounts

Using User Accounts feature, you can manage users. You can add a new user and also perform specific action on existing users. For example, resending verification email, reset a password, and delete a user. You can also use the Manage Saved Search option to perform collective action on users. Using the search option, you can find user according to the selected filters - such as Status, Is blocked and role - and save the search results. For more information, view how to manage saved search.

Notes:

- Using this option, you cannot manage your own details. You can only manage the users that you add. To reset your password, navigate to User Profile.
- To enable two-factor authentication (2FA) requirement for the users that you have added, see How to Enable 2FA Requirement at Organization Level.
- To disable two-factor authentication (2FA) requirement for the users that you have added, see How to Disable 2FA Requirement at Organization Level.

For list of global and individual actions, view following links:

- How to Perform Common Individual and Global Actions
- How to perform individual actions for Cloud Hybrid
- How to perform global actions for Cloud Hybrid
- How to perform individual actions for Cloud Direct
- How to perform global actions for Cloud Direct

What's next!

- View and Update User Account
- Add a User

How to View and Update User Account

Arcserve® Business Continuity Cloud lets you view and perform multiple actions on user accounts. From User Accounts screen, you can search users, view details and perform multiple actions on the existing accounts.

Key Actions Performed on User Accounts:

- **Search User Accounts:** Enter a search term or use desired filters in the search box to search an account. You can save the search and also manage saved search.
- **View User Account Details:** The User Accounts screen displays all the added user accounts with specified details set using the Settings icon. For example, Email, role, last logged on, Is Blocked, and so on.
- **Delete User Account:** Select multiple accounts and select delete from drop-down option of **Actions** to delete multiple accounts together. To delete one user account, click the drop-down arrow placed in user account details and click **Delete**. A Confirmation dialog is displayed. Click **Confirm** to delete.
- **Reset Password:** The option appears for those existing users whose status displays verified. Clicking **Reset Password** option from the drop-down list of selected user results in a Confirmation dialog. Click **Send Email** to confirm reset password and a link is sent to the registered email ID of selected user.

  Note: After sending the Reset Password link, the user cannot log into the Console using the old password.
- **Reset Two Factor:** To disable two-factor authentication for a particular user, select the **Reset Two Factor** option from the Action drop-down list. The confirmation message appears asking you to disable two-factor authentication. Click **Reset User Two Factor** to confirm.

  Note: After the two factor is reset, 2FA gets disabled.
- **Resend Verification Mail:** The option appears for those users who are added but not verified. Click **Resend Verification Email** from the drop-down list of selected user. A confirmation message informs that the email was sent to the email ID of the selected user.
- **Add a user:** From the User Accounts screen, click the option to add a user. For details, view How to add a user.

How to Add a User

From the User Account screen, you can add a new user and assign role.

Follow these steps:

1. Click **Add User**.

   Add User dialog is displayed.

2. Enter the following details:

   - **First Name** and **Last Name**: Enter full name of user
   - **Email Address:** Enter the email address of user. Email address cannot be reused for other user. The verification email is sent to the provided email ID. To get verified, the new user needs to click the activation link sent to the provided email. After successful verification, the user is assigned a role and then only user can perform any action. Without clicking the activation link shared in the verification email to create password, the user remains unverified and cannot log into the Cloud Console.
   - **Role:** Select a role to assign the new user. For example, Admin.

3. Click **Add User**.

   Add User dialog closes and the new user is displayed at the User Account screen.

Manage Roles

From Roles screen, you can view details about the active role.

Key Highlights:

- Expand the name of role to view permissions assigned to the role.
- View number of users who have the role assigned.
- View description about a role.

Chapter 7: Using Arcserve® Business Continuity Cloud as Direct Monitor

Using Arcserve® Business Continuity Cloud, a Direct monitor can apply filters and view jobs, logs, and reports.

This section contains the following topics:

Dashboard

After logging into Arcserve® Business Continuity Cloud, you land on the Console dashboard where you can view multiple common options and the details of Monitor feature. From the Dashboard, you can change password, update user details, view details to contact support, view important messages and log out.

Dashboard provides the following options:

- **Arcserve Icon:** Click on the Arcserve icon, placed on the top-left corner, and return to dashboard from anywhere in the Console.
- **Help Icon:** The Help icon on top-right takes you to the **Support** page where you can opt from multiple options to contact Arcserve and view Online help for the Console.
- **Alert Icon:** The exclamation mark icon on top-right displays messages from the Console for your consideration. The messages are categorized as **Critical**, **Warning** or **Information**. You can Acknowledge the messages and take action when required. For more details, view How to Manage Alerts.
- **User Login Icon:** The icon on top-right corner displays the profile picture of the logged-in user. The icon provides option to log out from Cloud Console and update user profile of the logged-in user.

Using User Profile, you can make two updates:

- **Update Contact Information:** From **My Profile** screen, you can update your contact details and upload photo. Click **Save Changes** after making updates.
- **Change Password:** Provide a new password and click **Update Password**.
- **Two-Factor Authentication:** Provide the current password, and then do one of the following:
  - To enable two-factor authentication, click **Enable Two Factor Authentication**.
  - To disable two-factor authentication, click **Disable Two Factor Authentication**.
  - To generate two-factor codes, click **Generate Two Factor Codes**.

Monitor

After logging into Arcserve® Business Continuity Cloud, you land on the Console dashboard where Monitor displays the details of your product using multiple wizards. From the Monitor, you can perform the following options:

- **View Summary:** Monitor displays Source Summary, Usage Summary and Policy Summary for the organization.
  - **Source Summary:** Displays the count of Total Sources and the count of sources with Protected, Offline or Unprotected status based on the last backup job result.
  - **Usage Summary:** Displays the usage summary of licensed capacity for Cloud Direct or Cloud Hybrid.
  - **Policy Summary:** Displays the count of Total Policies and the count of policies with Success, Deploying, Failure or Disabled status.
- **View Details as Graphs:** For better monitoring of key details, Monitor displays graphical view of multiple fields. For example:
  - **Backup Job Summary:** Displays the last 24 hours Backup Job count for Finished, Canceled, or Failed status. Hover over the graph to view the percentage for each status.
  - **Recent 10 Jobs in Progress:** Displays recent 10 jobs in progress, supports view log or cancel job action for all *in progress* job. Clicking **View all jobs** link leads you to the Jobs screen.
  - **Top 10 Sources:** Display top 10 sources per specific condition. Supports selected Backup Job Status, Events, Job Durations, and Data Transferred.
  - **Top 10 Polices:** Displays top 10 policies and group by Job status as Finished, Failed, Canceled, or Active.
  - **Usage Trend for Cloud Direct Volumes:** Displays Usage Trend for Cloud Direct Volumes by Full backup data and group by volume name.
  - **Usage Trend for Cloud Hybrid Stores:** Displays Usage Trend for Cloud Hybrid Stores and group by Cloud Hybrid Store name.
  - **Data Transfer Summary For Cloud Direct Volumes:** Displays Data Transfer Summary for Cloud Direct Volumes and group according to Data Processed, Data Transferred, or Data Written.

- **Dedupe Savings Trends For Cloud Hybrid Stores:** Displays Dedupe Savings Trends For Cloud Hybrid Stores and group by Source Data or Dedupe Savings size.

- **View Cloud Hybrid Details:** View usage trend and dedupe savings trend for Cloud Hybrid Stores. Hover over the graph to view details.
- **Expand or Collapse widgets:** Use the icon placed above a displayed widget to expand or collapse.

Analyze

The Analyze feature lets you view Jobs, Log, and Reports. The icon on top lets you collapse or expand the screen.

What's Next!

- Analyze Jobs
- Analyze Logs
- Analyze Reports

Analyzing Jobs

Displays complete list of jobs with the details that you can view.

Key Highlights

- The search bar helps you find a job according to the selected filters. For example, status, job type, date range or protection policy.
- You can save the search also for future usage.
- Manage Saved Search option lets you manage a search if you have saved.
- All the jobs display details that you can customize by using the Settings icon. Jobs are divided into multiple categories based on status. For example, Jobs in Progress, Failed Jobs, Canceled Jobs, and Successful Jobs.
- View Job description, such as Name of job, type of job, status of job, policy associated with source, destination of recovery point, duration, start and end time of job. You can also view the job description from the Jobs tab on the screen of a source.
- For every job, you can **view log**. Click the drop-down option placed at the end of every row of a job to view log of that job.

Analyzing Logs

The log tab displays all activity logs for the protected nodes. You can view logs and apply various filters such as severity, logs generated from the machine, job type, and log content. You can also Export logs. Message ID provides a hyperlink to access detailed documentation. Click the hyperlink in the MessageID column to view the description and solution for that message. On the log screen, Message IDs are displayed only for Replication IN jobs.

Export Logs: From the Log screen, you can export the logs to your Inbox. Click **Export** from the top of Log screen and the log is sent to your registered email ID. In your inbox, find the email from Arcserve Cloud Support email with the subject Log Export and click **Download Export** in the email to download log as .csv file.

Search Logs: You can search the activity logs using a combination of the available filters or one of the following options and clicking **Search**:

- Select **Severity** types to view all the logs related to the selected type.
- Select **Job Type**.
- Select **Date Range**.
- Select **Generated From** location.
- Enter message term in the Search box.

Analyzing Alert Reports

Use Arcserve® Business Continuity Cloud to analyze alerts separately or together based on the alert type.

From the list of alerts, you can view alert details such as Alert Name, Alert Type, Report for, Created on, Last Generated, and Recipients.

Analyzing Reports

Arcserve® Business Continuity Cloud helps you analyze the report together as well as separately according to the report types. From the Report screen, you can search for reports using the filters of Date Range, Schedule for, and Generate on. Also, you can save the search item.

From the list of reports, you can view details about a report. For example, Report Name, Date Range, Report for, Generated on, Scheduled for, Report type, Created by, and Recipients. From the report screen and related screens, you can also perform following actions:

- View Reports
- Manage Report Schedules
- Export report

How to View a Report

Using the Console, you can view reports directly from the Report screen or navigate to a specific type to view related reports. From the report screen, you can perform the following actions:

- **View Details of Report:** The list of report displays all the reports including Backup Jobs reports, Recovery Jobs reports, Data Transfer reports, and Capacity Usage reports. You can use Search bar to filter the type of reports to view. Clicking the report name lets you view complete details in dashboard.
- **View Reports of Specific Type:** To view specific reports of only one type, navigate to any of the available report types. From report screen of specific types, you can also export the report.

Available Report types:

- Backup Jobs
- Policy Tasks
- Recovery Jobs
- Data Transfer
- Capacity usage

Report for Backup Jobs

From the console, click Backup Jobs below Reports to reach the screen that lets you view summary of all the backup jobs. You can also search the source using the filters of Date Range, Protection Policy, Destination or Source Groups. Using multiple filters is allowed.

Key Highlights:

- From the screen, you can Export Report as .csv file.
- Hover over the chart to view percentage of Failed, Finished, and Canceled jobs.
- View top 10 sources and filter according to Backup Job Status, Events, Jobs Duration or Data Transferred.
- Hover over the graph to view classification of Finished, Failed and Canceled jobs.
- View **Details** of all backup jobs from the table.

Report for Policy Tasks

To view the policy tasks details of completed backup jobs, go to **Analyze** > **Policy Tasks**.

Click **Policy Tasks** to view the summary of the policy tasks of completed backup jobs. You can search the source using multiple filters such as Date Range, Protection Policy, Destination, and Sources Groups. On the top-right corner of the **Policy Tasks** page, click **Manage Saved Searches** and select an option that you want to view in the report.

Key Highlights

- From the screen, you can export report as a .csv file.
- Hover over the chart to view the percentage of Finished, Failed, and Canceled jobs.
- Apply filters to view Top 10 Sources such as Events and Job Duration.
- Hover over the graph to view classification of Finished, Failed, and Canceled jobs.
- From the table, view Details of all policy tasks for completed backup jobs.

Report for Recovery Job

From the Console, click Recovery Jobs below Reports to reach the screen that lets you view summary of all the jobs recovered. You can also search the source using the filters of Date Range, Destination or Source Groups. Click icon of Settings to select the option that you want to view in report.

Key Highlights:

- Hover over the chart to view percentage of Failed, Canceled, and Finished jobs.
- View top 10 sources and filter according to Recovery Job Status, Events, Jobs Duration or Data Transferred.
- Hover over the graph to view classification of Finished, Failed, and Canceled jobs.
- View **Details** of all restore jobs from the table.
- Export the reports as CSV file.
- Manage saved search.

Report for Data Transfer

From the console, click Data Transfer below Reports to reach the screen that lets you view summary of data transfer. You can also search the source using the filters of Date Range and Source Groups.

Key Highlights:

- Hover over the chart to view data processed, data transferred and data written on a specific date.
- Hover over the graph to view classification of Finished, Failed and Canceled jobs.
- View **Details** of all data transfer from the table.
- Export the reports as CSV file.
- Manage saved search.

Report for Capacity Usage

From the console, click Capacity Usage below Reports to reach the screen that lets you view usage trends and dedupe savings trend. You can also search the destination using the filters of Date Range, and Destination.

Key Highlights:

- Hover over the chart to view usage trend and dedupe saving trend on different dates.
- View **Details** of capacity usage from the table.
- View details about all available destinations.
- Export the reports as CSV file.
- Manage saved search.

Manage Report Schedules

You can manage schedules of all the report using Manage Report Schedules. Under Analyze>Reports, click Manage Report Schedules and you can view list of all reports. From the screen, you can perform the following actions:

- **Search:** To search reports, either provide a report name in the search bar or use filters of **Scheduled for** and **Report Type**.
- **View details:** The list of report provides complete details about every report. For example, Report Name, Report Type, Report for, Scheduled For, Created by, Created on, Last Generated.

Chapter 8: Using Arcserve® Business Continuity Cloud as MSP Monitor

Using Arcserve® Business Continuity Cloud for MSP and MSP-based organizations, an MSP monitor can apply filters and view jobs, logs, and reports.

This section contains the following topics:

Dashboard

After logging into Arcserve® Business Continuity Cloud, you land on the Console dashboard where you can view multiple common options and the details of Monitor feature. From the Dashboard, you can change password, update user details, view details to contact support, view important messages and log out.

Dashboard provides the following options:

- **Arcserve Icon:** Click on the Arcserve icon, placed on the top-left corner, and return to dashboard from anywhere in the Console.
- **Help Icon:** The Help icon on top-right takes you to the **Support** page where you can opt from multiple options to contact Arcserve and view Online help for the Console.
- **Alert Icon:** The exclamation mark icon on top-right displays messages from the Console for your consideration. The messages are categorized as **Critical**, **Warning** or **Information**. You can Acknowledge the messages and take action when required. For more details, view How to Manage Alerts.
- **User Login Icon:** The icon on top-right corner displays the profile picture of the logged-in user. The icon provides option to log out from Cloud Console and update user profile of the logged-in user.

Using User Profile, you can make two updates:

- **Update Contact Information:** From **My Profile** screen, you can update your contact details and upload photo. Click **Save Changes** after making updates.
- **Change Password:** Provide a new password and click **Update Password**.
- **Two-Factor Authentication:** Provide the current password, and then do one of the following:
  - To enable two-factor authentication, click **Enable Two Factor Authentication**.
  - To disable two-factor authentication, click **Disable Two Factor Authentication**.
  - To generate two-factor codes, click **Generate Two Factor Codes**.

Monitor

After logging into Arcserve® Business Continuity Cloud, you land on the Console dashboard where Monitor displays the details of your product using multiple wizards. From the Monitor, you can perform the following options:

- **View Summary:** Monitor displays summary of customer, usage, and source for the organization.
  - **Customer Summary:** Displays the count of Total customers and the count of customers with Failed and Success status based on the job result of last backup.
  - **Usage Summary across customers:** Displays the usage summary of customers according to the licensed capacity for Cloud Direct or Cloud Hybrid.
  - **Source summary across customers:** Displays the count of sources of all customers according to the status. For example, protected, not protected and offline.
- **View Details as Graphs:** For better monitoring of key details, Monitor displays graphical view of multiple fields. For example:
  - **Backup Job Summary:** Displays the last 24 hours Backup Job count for Finished, Canceled, or Failed status. Hover over the graph to view the percentage for each status.
  - **Recent 10 Jobs in Progress:** Displays recent 10 jobs in progress, supports view log or cancel job action for all *in progress* job. Clicking **View all jobs** link leads you to the Jobs screen.
  - **Top 10 Sources:** Display top 10 sources per specific condition. Supports selected Backup Job Status, Events, Job Durations, and Data Transferred.
  - **Top 10 Polices:** Displays top 10 policies and group by Job status as Finished, Failed, Canceled, or Active.
  - **View Top 10 Customers:** Helps you monitor Top 10 customers of MSP user.
  - **Usage Trend for Cloud Direct Volumes:** Displays Usage Trend for Cloud Direct Volumes by Full backup data and group by volume name.
  - **Usage Trend for Cloud Hybrid Stores:** Displays Usage Trend for Cloud Hybrid Stores and group by Cloud Hybrid Store name.

- **Data Transfer Summary For Cloud Direct Volumes:** Displays Data Transfer Summary for Cloud Direct Volumes and group according to Data Processed, Data Transferred, and Data Written.
- **Dedupe Savings Trends For Cloud Hybrid Stores:** Displays Dedupe Savings Trends For Cloud Hybrid Stores and group by Source Data and Dedupe Savings size.

- **View Cloud Hybrid Details:** View usage trend and dedupe savings trend for Cloud Hybrid Stores. Hover over the graph to view details.
- **Expand or Collapse widgets:** Use the icon placed above a displayed widget to expand or collapse.

Analyze

The Analyze feature lets you view Jobs, Log, and Reports.

- Analyze Jobs
- Analyze Logs
- Analyze Reports

Analyzing Jobs

Displays complete list of jobs with the details that you can view.

Key Highlights

- The search bar helps you find a job according to the selected filters. For example, status, job type, date range or protection policy.
- You can save the search also for future usage.
- Manage Saved Search option lets you manage a search if you have saved.
- All the jobs display details that you can customize by using the Settings icon. Jobs are divided into multiple categories based on status. For example, Jobs in Progress, Failed Jobs, Canceled Jobs, and Successful Jobs.
- View Job description, such as Name of job, type of job, status of job, policy associated with source, destination of recovery point, duration, start and end time of job. You can also view the job description from the Jobs tab on the screen of a source.
- For every job, you can **view log**. Click the drop-down option placed at the end of every row of a job to view log of that job.

Analyzing Logs

The log tab displays all activity logs for the protected nodes. You can view logs and apply various filters such as severity, logs generated from the machine, job type, and log content. You can also Export logs. Message ID provides a hyperlink to access detailed documentation. Click the hyperlink in the MessageID column to view the description and solution for that message. On the log screen, Message IDs are displayed only for Replication IN jobs.

Export Logs: From the Log screen, you can export the logs to your Inbox. Click **Export** from the top of Log screen and the log is sent to your registered email ID. In your inbox, find the email from Arcserve Cloud Support email with the subject Log Export and click **Download Export** in the email to download log as .csv file.

Search Logs: You can search the activity logs using a combination of the available filters or one of the following options and clicking **Search**:

- Select **Severity** types to view all the logs related to the selected type.
- Select **Job Type**.
- Select **Date Range**.
- Select **Generated From** location.
- Enter message term in the Search box.

Analyzing Alert Reports

Use Arcserve® Business Continuity Cloud to analyze alerts separately or together based on the alert type.

From the list of alerts, you can view alert details such as Alert Name, Alert Type, Report for, Created on, Last Generated, and Recipients.

Analyzing Reports

Using the Console, you can view four types of reports: Backup Jobs, Recovery Jobs, Data Transfer, and Capacity Usage. Search bar lets you find a report using filter criteria such as Generated on, Scheduled for, and Date Range. You can view reports about Backup and Recovery Jobs, Data Transfer, and Capacity Usage. You can also export reports as .csv file.

- View Reports
- Manage Report Schedules
- Export report

How to View a Report

Using the Console, you can view reports directly from the Report screen or navigate to a specific type to view related reports. From the report screen, you can perform the following actions:

- **View Details of Report:** The list of report displays all the reports including Backup Jobs reports, Recovery Jobs reports, Data Transfer reports, and Capacity Usage reports. You can use Search bar to filter the type of reports to view. Clicking the report name lets you view complete details in dashboard.
- **View Reports of Specific Type:** To view specific reports of only one type, navigate to any of the available report types. From report screen of specific types, you can also export the report.

Available Report types:

- Backup Jobs
- Policy Tasks
- Recovery Jobs
- Data Transfer
- Capacity usage

Report for Backup Jobs

From the console, click Backup Jobs below Reports to reach the screen that lets you view summary of all the backup jobs. You can also search the source using the filters of Date Range, Protection Policy, and Destination. Using multiple filters is allowed.

Key Highlights:

- From the screen, you can Export Report as .csv file.
- Hover over the chart to view percentage of Failed, Finished, and Canceled jobs.
- View top 10 sources and filter according to Backup Job Status, Events, Jobs Duration or Data Transferred.
- Hover over the graph to view classification of Finished, Failed and Canceled jobs.
- View **Details** of all backup jobs from the table.

Report for Policy Tasks

To view the policy tasks details of completed backup jobs, go to **Analyze** > **Policy Tasks**.

Click **Policy Tasks** to view the summary of the policy tasks of completed backup jobs. You can search the source using multiple filters such as Date Range, Protection Policy, Destination, and Organizations. On the top-right corner of the **Policy Tasks** page, click **Manage Saved Searches** and select an option that you want to view in the report.

Key Highlights

- From the screen, you can export report as a .csv file.
- Hover over the chart to view the percentage of Finished, Failed, and Canceled jobs.
- Apply filters to view Top 10 Sources such as Events and Job Duration.
- Hover over the graph to view classification of Finished, Failed, and Canceled jobs.
- From the table, view Details of all policy tasks for completed backup jobs.

Report for Recovery Jobs

From the Console, click Recovery Jobs below Reports to reach the screen that lets you view summary of all the jobs restored. You can also search the source using the filters of Date Range, Destination, and Organization. Click icon of Settings to select the option that you want to view in report.

Key Highlights:

- Hover over the chart to view percentage of Failed, Canceled, and Finished jobs.
- View top 10 sources and filter according to Recovery Job Status, Events, Jobs Duration or Data Transferred.
- Hover over the graph to view classification of Finished, Failed and Canceled jobs.
- View **Details** of all recovery jobs from the table.
- Export the reports as CSV file.
- Manage saved search.

Report for Data Transfer

From the console, click Data Transfer below Reports to reach the screen that lets you view summary of data transfer. You can also search the source using the filters of Date Range.

Key Highlights:

- Hover over the chart to view data processed, data transferred and data written on a specific date.
- Hover over the graph to view classification of Finished, Failed and Canceled jobs.
- View **Details** of all data transfer from the table.
- Export the reports as CSV file.
- Manage saved search.

Report for Capacity Usage

From the console, click Capacity Usage below Reports to reach the screen that lets you view usage trends and dedupe savings trend. You can also search the destination using the filters of Date Range, and Destination.

Key Highlights:

- Hover over the chart to view usage trend and dedupe saving trend on different dates.
- View **Details** of capacity usage from the table.
- View details about all available destinations.
- Export the reports as CSV file.
- Manage saved search.

Manage Report Schedules

You can manage schedules of all the report using Manage Report Schedules. Under Analyze>Reports, click Manage Report Schedules and you can view list of all reports. From the screen, you can perform the following actions:

- **Search:** To search reports, either provide a report name in the search bar or use filters of **Scheduled for** and **Report Type**.
- **View details:** The list of report provides complete details about every report. For example, Report Name, Report Type, Report for, Scheduled For, Created by, Created on, Last Generated.

Protect

The Protect feature lets you view the list of customers.

This section contains the following topics:

How to Search, View, and Perform Multiple Actions on Customer Account

The customer accounts screen provides the details of the customer accounts.

Search an account: From the search bar, find customer accounts using the name of the customers.

View account details: The customer accounts screen displays the list of all available customer accounts. For each account, view details such as Customer Name, Status, Account State, Total Sources, Product Usage, Added by and Added on.

View Count of Accounts: On the top-right corner of the page, **Total Customer Accounts** displays the number of customer accounts added.

View Count of Accounts Suspended: On the top-right corner of the page, **Total Customer Accounts Suspended** displays the number of customer accounts suspended.

View as End-User Admin: To switch the user role and view the Monitor and Analyze screens, do one of the following:

- Next to the name of a customer account, click the icon  .
- From the **Action** drop-down list of a customer account, click the **View as End-User Admin** option.

Chapter 9: Working With Arcserve® Business Continuity Cloud

The section contains the following topics:

How to Recover or Pin a Recovery Point

You can recover or pin a recovery point. From the recovery point tab of a destination, click the drop-down option for action. Pin or Recover option appear.

Pin a Recovery Point: Using the Pin option keeps a recovery point highlighted. If you select **Pin** from the drop-down option of a recovery point, the icon at start turns yellow.

Recover a Recovery Point: To recover, you need to perform two steps in the Restore Wizard.

Follow these steps:

1. Click the name of a destination or click **View Recovery Point** from the drop-down option of a destination displayed in the list of Destinations screen.

   You are led to the detailed page of selected destination and the **Recovery Points** tab displays full list.

2. Select a recovery point and click **Recover** from the drop-down option available at the end of details.

   The Restore wizard is displayed.

3. As Step 1, you can **Specify Recovery Point**, **Update the Image** format or **Destination path** and click **Next**.

4. In Step 2, use **Select Target Machine** to select a target machine and click **Restore**.

   Note: The machines are displayed only if you select the radio button of Restore on to another machine. To restore on the source machine, select the radio button of **Restore on the original source machine** and click **Restore**.

   A message confirms that recovery started successfully and you return to the selected destination.

From the Specify Recovery Point tab, you can also **Browse Recovery Point** to restore using Cloud Direct Agent. When you click **Browse Recovery point**, the Browse Recovery Point dialog appears displaying folders with details. You can perform the following actions:

- **Show/Hide Folders panel:** Displays or hides the complete folder structure of the volume based on your selection.
- **Restore:** To restore, select one file/ folder and click **Restore Using Cloud Direct Agent**.

- **Refresh:** Click the **Refresh** icon on top to get the latest information on Recovery points.
- **Views:** Customize the views of folders according to your requirement. You can customize to view details or view folder names only in desired size.

How to Recover a Recovery Point for Cloud Direct

You can recover a recovery point. From the recovery point tab of a destination, select check box of displayed recovery point and click the drop-down option for action. The Recover option appear. You can find a source either from the **Sources** or **Destinations** tab available under **Protect** feature.

Considerations for Recovery:

- Recovery option appears for a source only when at least one successful backup is complete for that source.
- The exclude option is available when the Activity Type selected is Cloud Direct file folder.

Recover a Recovery Point: To recover, you need to perform two steps in the Restore Wizard.

Follow these steps:

1. To recover, perform one of the following options:

   From the Source screen:

   - Click the name of a source

     or

   - Select the check box of a Source and click **Start Recovery** from the drop-down option of the selected Source.

   From the Destinations Screen:

   - Click the name of a source.

     or

   - Click **View Recovery Point** from the drop-down option of a Source displayed in the list of Destinations screen.

   You are led to the detailed page of selected source or destination and the **Recovery Points** tab displays full list.

2. Select a recovery point and click **Recover** from the drop-down option available at the end of details.

   Considerations:

   - If your source is an Agentless Machine or Windows Image Backup recovery point, click **Browse Recovery Point** and select the .img file associated with each disk of your Agentless Machine.

- If your disk is a static NTFS format drive (likely on a Windows system), you can double click on the .img file and select a folder or file on the disk. Then, click **Restore Using Cloud Direct Agent**.
- If you selected an .img file, select a format to convert your .img file. Mac, Windows, and Linux can restore as vhdx. Linux 64 bit can also restore as vmdk.

- If you selected a Folder or SQL backup task point, click **Browse Recovery Point**, navigate to the file or folder you want to recover and click **Restore Using Cloud Direct Agent**.
- If you clicked Browse Recovery Point, you can right click on any file that is less than 140 MB and click **Download**. As the option is a result of a browser download, none of the original ACLs and timestamps are preserved.
- If you selected a File backup, then you can just enter the destination path.

The Restore wizard is displayed.

3. As Step 1, you can **Specify Recovery Point**, **Update the Image** format or **Destination path** and click **Next**.

   Considerations:

   - Verify if the destination path is a valid path for the destination system where you will recover to.
     - For Windows destinations, you can enter local drive or UNC paths if you selected a folder. If you selected a .img or file and want to recover to a Windows system, enter a local drive path.
     - For Linux or Mac destinations you can enter a Linux path.
   - If a folder is selected, the CD Agent will recover the contents of the selected folder into the path entered. If you would like to restore the selected folder with the same name, enter the folder name at the end of the destination path.

4. In Step 2, use **Select Target Machine** to select a target machine and click **Restore**.

   Considerations:

   - If you want to restore a file/folder from a Windows source or SQL backup, select a Windows source as a destination.

- If you want to restore a file/folder from a Mac or Linux source, please select a Mac or Linux source as a destination.

Note: The machines are displayed only if you select the check box of Restore on to another machine. To restore on the source machine, select the check box of **Restore on the original source machine** and click **Restore**.

A message confirms that recovery started successfully and you return to the selected destination.

How to Download File / Folder from a Recovery Point

You can download file or folder from a recovery point.

Supported Source Nodes: Windows/Linux Agents, Windows/Linux Agentless, CIFS/NFS source nodes.

Follow these steps:

1. From the Modify Destination screen, click the **Recovery Points** tab.

   List of Sources is displayed.

2. Expand a source.

   List of recovery points is displayed.

3. From the drop-down arrow of a recovery point, click **Download File/Folder**.

   If session is encrypted, the Protected Password dialog is displayed. Then, you need to perform Step 4.

   If session is not encrypted, the Browse Recovery Point screen appear. Then, you can move to Step 5.

4. (Optional) Enter **Password** in the **Protected Password** dialog and click **Browse**.

   Browse Recovery Point screen appears.

5. From the **Browse Recovery Point** screen, perform the following steps:

   a. Expand / click the file tree in the left pane.

   b. Select checkboxes of desired files / folders from the list of recovery points displayed.

   c. Click **Download**.

      A confirmation message informs about the status of download.

   The file or folder of recovery point is downloaded.

   Note: SQL Server files/folder download is not supported.

How to Configure Reverse Replication to a New Recovery Points Server for Cloud Hybrid

Important! When replicating data from Cloud Hybrid to On-premise RPS server, do not select the source Console/RPS Server as your replication destination. To avoid data corruption, we recommend using a new Console/RPS Server.

Adding a policy for Arcserve® Business Continuity Cloud involves three main steps.

Follow these steps:

1. Set up a new server and install Arcserve UDP Console and RPS server.

   Notes:

   - Verify that the Arcserve UDP Console and Agent ports are open and accessible from Internet that helps to establish the connection to Cloud Hybrid and RPS.
   - Default Ports: 8014/8015
   - For better security, we recommend to install using the HTTPS protocol.

2. Create a deduplication data store, enable encryption, and set the deduplication block size to 16 KB for better performance.

   Note: Enable the data store for deduplication and encryption.

3. Create a local non-administrator user and a shared replication plan.

   For more information, refer link.

4. Log into the Arcserve Cloud Console using the credentials from Arcserve Cloud.
5. Navigate to Protect>Policies, select the node(s) where you need to perform reverse replication, and modify the corresponding policy.
6. Click the third tab - **Destination** where you need to define the policy in detail.

   You need to configure policy to add a task for Replicate to a remotely-managed RPS.

7. Perform the following steps and add a Replicate to a remotely-managed RPS task:

   - Click the cross icon to close the Replicate from a remotely-managed RPS task.
   - Click the Hyperlink icon to add a Replicate to a remotely-managed RPS task.
   - Click the **Replicate to a remotely-managed RPS** task.
   - In the tab, **What to protect**, select desired activity

8. In the tab, **Where to protect**, provide remote UDP Console access information to get share plan.
9. (Optional) In the tab, **When to protect**, add Replicate Schedule.
10. Click **Save Policy**.

    The policy updates are saved.
11. Perform the replication job in the Cloud Console using one of the following options:

    Note: We recommend Option A.

    - Option A: Trigger replication job manually, navigate to Protect>Sources, and click **Start Replication** action.
    - Option B: Waiting for scheduled replication job running on the start time of time range that is provided in step 9.
    - Option C: Waiting for backup job to trigger if any replication schedule is not provided.
12. Perform the restore job such as BMR, VM recovery, IVM as required in the Arcserve UDP Console.

How to Create a New Report

Using Create Reports, you can add a new report. You can create new report directly while viewing a specific type of report screen also. The report is sent as a link to the email ID and the additional recipients if added. Create report wizard is required to create a new report. The wizard appears when you click **Create Report** on the Report screen.

Follow these steps:

1. From the Analyze screen, click the **Report** tab.

   Report screen is displayed.

2. From the Report screen, click **Create Report**.

   Create Report wizard appears.

3. From the **Create Report** wizard, select one of the options from **Report Type**.
4. Enter a unique name for your new report in the **Report Name** field.
5. Select one of the options:

   - **Report all Sources:** Lets you generate report from all available sources.
   - **Report selected Source Groups:** Lets you generate report only from the selected source groups. If you select this option, also select Source group from the drop-down option and click Add. Repeat the action to select multiple groups.

6. (Optional) To share your report with others, enter email ID of one or more recipients and click **Add**.
7. Select one of the options to create report:

   - **Generate Report now:** Lets you create and email report immediately. If you opt for this option, then select a duration from the drop-down option of Select a date range for the report. The date range is of the same day (Last 24 hours), last 7 days or last 1 month. You can also use custom to select your choice of date range.
   - **Set a Schedule:** lets you plan to create and email report later. If you opt to schedule, provide the Delivery Time and Frequency. Based on your selection, report is shared through email daily, weekly or monthly.

   If all the fields are entered properly, Create button is enabled.

8. Click **Create**.

   The confirmation dialog informs about successful generation of the report.

Successful creation of report results into report getting listed on the **Report** screen and an email sent to the logged in user and other recipients (if added). From the report screen or respective report type screen, you can view all the reports.

How to Edit a Report Schedule

You can edit a report schedule using the Manage Report Schedule option.

Follow these steps:

1. Navigate to the Analyze screen, click **Reports>Manage Report Schedule**.

   List of reports is displayed on Manage Report Schedule screen.

2. From the list, click either the name of a Report or from the drop-down option of a Report click **Edit**.

   Edit Report Settings screen is displayed.

3. From the screen, select one of the options to specify sources:

   - **Report all Sources:** Lets you edit report from all available sources.
   - **Report selected Source Groups:** Lets you modify report only from the selected source groups. If you select this option, also select Source group from the drop-down option and click **Add**. Repeat the action to select multiple groups.

4. To share your report with others, enter email ID of one or more recipients and click **Add**.

5. Modify schedule using options., such as, Provide the Delivery Time and Frequency. Based on your selection, report is shared through email daily, weekly or monthly.

6. Click **Save Changes**.

   The report is modified.

How to Export a Report

You can export all the types of report using Export option from the specific report screen.

Follow these steps:

1. From Analyze>Reports, navigate to one of the report types - Backup jobs, Recovery jobs, Data Transfer or Capacity Usage.

   Selected report type screen is displayed.

2. From the screen, click **Export Report as** and then click **.CSV**.

   A confirmation message appears to inform that the report is sent to your registered email ID.

3. From your registered Email ID, open the email from Arcserve Support and click **Download Export.**

   The report is downloaded as .csv file.

How to Create a New Report (MSP Admin)

Using Create Reports, you can add a new report. You can create new report directly while viewing a specific type of report screen also. The report is sent as a link to the email ID and the additional recipients if added. Create report wizard is required to create a new report. The wizard appears when you click **Create Report** on the Report screen.

Follow these steps:

1. From the Analyze screen, click the **Report** tab.

   Report screen is displayed.

2. From the Report screen, click **Create Report**.

   Create Report wizard appears.

3. From the **Create Report** wizard, select one of the Report options from **Report Type**.
4. Enter a unique name for your new report in the **Report Name** field.
5. Select one of the options:

   - **Report all Organization:** Lets you generate report from all available organizations.
   - **Report selected Organizations:** Lets you generate report only from the selected organizations. If you select this option, also select Organization from the drop-down option and click Add. Repeat the action to select multiple organizations.

6. (Optional) To share your report with others, enter email ID of one or more recipients and click **Add**.
7. Select one of the options to create report:

   - **Generate Report now:** Lets you create and email report immediately. If you opt for this option, then select a duration from the drop-down option of Select a date range for the report. The date range is of the same day (Last 24 hours), last 7 days or last 1 month. You can also use custom to select your choice of date range.
   - **Set a Schedule:** lets you plan to create and email report later. If you opt to schedule, provide the Delivery Time and Frequency. Based on your selection, report is shared through email daily, weekly or monthly.

   If all the fields are entered properly, Create button is enabled.

8. Click **Create**.

   The confirmation dialog informs about successful generation of the report.

Successful creation of report results into report getting listed on the **Report** screen and an email sent to the logged in user and other recipients (if added). From the report screen or respective report type screen, you can view all the reports.

How to Manage Saved Search

You have performed a search and saved. Later you want to perform an action that applies to a saved search. How can you do that?

Arcserve® Business Continuity Cloud lets you manage your saved search. Using the feature, you can perform multiple actions on a saved search to update and also helps you delete a saved search.

Follow these steps:

1. From the drop-down option of icon  , click **Manage Saved Searches**.

   Manage Saved Searches dialog appears displaying names of all save searches for that feature.

2. For **Sources**, from the list of Saved Searches select the name that you want to manage and perform update in one or more fields:

   Note: You cannot edit or delete an active filter.

   - **Saved Search Name:** Modify the name. If you select the check box of **Make as default table view**, the search name automatically applies for search when logged into organization.
   - **Message contains:** Replace the previous description.
   - **Protection Status:** Select status of protection: Protected or Not Protected
   - **Connection Status:** Select status of connection: Online or Offline.
   - **Backup Status:** Select the required status.
   - **OS:** Select an operating system from Windows, Linux or Mac.
   - **Source Groups:** Select a source group for saved search.
   - **Protection Policy:** Select a policy for saved search.

3. For tabs other than **Sources**, from the list of Saved Searches select the name that you want to manage and perform update in one or more fields:

   Note: You cannot edit or delete an active filter.

   - **Saved Search Name:** Modify the name. If you select the check box of **Make as default table view**, the search name automatically applies for search when logged into organization.
   - **Search String:** Replace the existing string.
   - **Date Range:** Select a date range.

- **Protection Policy:** Select a policy for saved search.
- **Destination:** Select a destination.
- **Source Groups:** Select a source group for saved search.

4. Click **Save** to update selected Saved Search.
5. (Optional) Click **Delete** to remove the Saved Search.

How to Perform Common Individual and Global Actions

You can perform multiple individual and global actions. For example, modify or delete policy, delete user, reset password and resend verification email to a user. Depending on the roles, the actions may vary. This topic describes how to perform some individual and global action for a function and helps you understand related prerequisites.

Sources

From Protect>Sources, you can perform multiple individual actions that vary according to your role.

Start Recovery

Click to start recovery of the source.

Prerequisites: Start Recovery option is visible only when the source meets following prerequisites:

- Not removed already
- At least one recovery point is available

Delete

Click to remove the selected source from Console. This action is performed as Individual and global both.

Prerequisites: After performing delete, the source is highlighted. Delete option is visible only when the source meets following prerequisites:

- Not deleted already
- No replication(in) job is active

Remove

Click to remove the selected source from Console. This action is performed as Individual and global both.

Prerequisite: Remove option is visible only when the source is already deleted.

Cancel Replication (In)

Click to cancel Replication(In) Job. This action is performed as Individual and global both.

Prerequisites: Cancel Replication (In) option is visible only when the source meets following prerequisites:

- Only Cloud Hybrid source is selected
- Not deleted already

- Replication(In) Job is running

Policies

From Protect>Policies, you can perform global actions that vary according to user role.

Modify

Click to update the Cloud Direct policy. This individual action is only applicable to one policy at a time.

Prerequisite: Modify option is visible only when the policy is not being deployed.

Delete

This option is used both as individual and global action. As global action, you can delete more than one policy together. As Individual action, you can delete only one policy at a time. Click to delete one or all selected policies.

Prerequisites when using as global action: Delete option is visible only when all the selected policies meet following prerequisites:

- Policy is not being deployed
- For Disaster Recovery policy, Recovered resources of Protected source are in deprovisioned state

Prerequisites when using as individual action: Delete option is visible only when the selected policy meet following prerequisites:

- Policy is not being deployed
- For Disaster Recovery policy, Recovered resources of Protected source are in deprovisioned state

User Accounts

From Configure>User Accounts, you can perform multiple global actions that vary according to user role.

Reset password

Click to reset password for all selected users.

Prerequisites: Reset password option is visible when following prerequisites are met:

- State shows verified
- Not selected own logged-in user ID

Resend Enrollment Email

Click to resend enrollment email to the selected users.

Prerequisite: Resend enrollment email option is visible only when the selected user(s) are in Unverified state.

Delete

This option is used both as individual and global action. As global action, you can delete more than one policy together. As Individual action, you can delete only one policy at a time. Click to delete one or all selected users.

Prerequisite: Delete option is visible only when you do not select the logged-in user.

Source Groups

From Configure>Source Groups, you can perform individual action that vary according to your role.

Delete Group

This option is used both as individual and global action. Click to delete one or more source groups.

How to Perform Individual Actions for Cloud Hybrid

You can perform multiple individual actions when using Cloud Hybrid. Depending on the roles, the actions may vary. This topic describes how to perform an individual action for a function and helps you understand related prerequisites.

Sources

From Protect>Sources, you can perform multiple individual actions that vary according to your role.

Start Recovery

Click to start recovery of the source.

Prerequisites: Start Recovery option is visible only when the source meets following prerequisites:

- Not removed already
- At least one recovery point is available

Start Replication

Click to start replication.

Prerequisites: Start Replication option is visible only when the source meets following prerequisites:

- Only Cloud Hybrid source is selected
- Not deleted already
- Assigned a policy that contains the task - Remote to a remotely-managed RPS

Delete

Click to remove the selected source from Console.

Prerequisites: After performing delete, the source is highlighted. Delete option is visible only when the source meets following prerequisites:

- Not deleted already
- No replication(in) job is active

Remove

Click to remove the selected source from Console.

Prerequisite: Remove option is visible only when the source is already deleted.

Cancel Replication (In)

Click to cancel Replication(In) Job.

Prerequisites: Cancel Replication (In) option is visible only when the source meets following prerequisites:

- Only Cloud Hybrid source is selected
- Not deleted already
- Replication(In) Job is running

Cancel Replication (Out)

Click to cancel Replication(Out) Job.

Prerequisites: Cancel Replication (Out) option is visible only when the source meets following prerequisites:

- Only Cloud Hybrid source is selected
- Not deleted already
- Replication(Out) Job is running or waiting

Destinations

From Protect>Destinations, you can perform multiple individual actions that vary according to your role.

Edit

Click to modify the Hybrid Store.

Prerequisite: Edit option is visible only when Hybrid Store is already not deleted.

View Recovery Points

Click to view recovery points of the Hybrid Store.

Prerequisite: View Recovery Points option is visible only when Hybrid Store is already not deleted.

Delete

Click to remove the Hybrid Store.

Prerequisites: Delete option is visible only when Hybrid Store meets the following prerequisites:

- Not in use by any policy
- No replication job is active
- No merge job is active

Policies

From Protect>Policies, you can perform multiple individual actions that vary according to your role.

Modify

Click to update the Cloud Hybrid policy.

Prerequisite: Modify option is visible only when the policy is not being deployed.

Delete

Click to delete the Cloud Hybrid policy.

Prerequisite: Delete option is visible only when the policy is not being deployed.

Jobs

From Analyze>Jobs, you can perform multiple individual actions that vary according to your role.

Cancel Job

Click to Cancel Replication(In) Job.

Prerequisite: Cancel Job option is visible for selection only when Replication (In) Job is running.

View Logs

Click to view Job Logs.

How to Perform Global Actions for Cloud Hybrid

You can perform multiple global actions when using Cloud Hybrid. Depending on the roles, the actions may vary. This topic describes how to perform a global action for a function and helps you understand related prerequisites.

Sources

From Protect>Sources, you can perform multiple global actions that vary according to your role.

Delete

Click to remove the selected source from Console.

Prerequisites: After performing delete, the source is highlighted. Delete option is visible only when the source meets following prerequisites:

- Not deleted already
- No replication-in job is active

Remove

Click to remove the selected source from Console.

Prerequisite: Remove option is visible only when the source is already deleted.

Cancel Replication (In)

Click to cancel Replication (In) Job.

Prerequisites: Cancel Replication (In) option is visible only when the source meets following prerequisites:

- Only Cloud Hybrid source is selected
- Not deleted already
- Replication(In) Job is running

Destinations

From Protect>Destinations, you can perform global actions that vary according to user role.

Delete

Click to remove the Hybrid Store.

Prerequisites: Delete option is visible only when Hybrid Store meets the following prerequisites:

- Not in use by any policy
- No replication job is active
- No merge job is active

Policies

From Protect>Policies, you can perform global action that varies according to user role.

Delete

Click to delete the Cloud Hybrid policy.

Prerequisite: Delete option is visible only when the policy is not being deployed.

Jobs

From Analyze>Jobs, you can perform global action that varies according to user role.

Cancel Job

Click to Cancel Replication(In) Job.

Prerequisite: Cancel Job option is visible for selection only when Replication (In) Job is running.

How to Perform Individual Actions for Cloud Direct

You can perform multiple individual actions when using Cloud Direct. Depending on the roles, the actions may vary. This topic describes how to perform an individual action for a function and helps you understand related prerequisites. For example, individual actions for Sources, Source Groups, Recovered Resources, Destinations, and Jobs.

Sources

From Protect>Sources, you can perform multiple individual actions that vary according to user role.

Upgrade Agent

Lets you upgrade Cloud Direct replication agent of the source.

Prerequisites: Upgrade Agent option is visible only when the source meets following prerequisites:

- Not deleted already
- Upgrade is available

Start Backup

Lets you start backup of the source.

Prerequisites: Start backup option is visible only when the source meets following prerequisites:

- Not deleted already
- A policy is available
- Recovered resource is not running
- An in-progress recovery job to restore data is not active

Cancel Backup

Lets you stop backup of the source.

Prerequisites: Cancel backup option is visible only when the source is not deleted already.

Start Recovery

Lets you start recovery of the source.

Prerequisites: Start Recovery option is visible only when the source meets following prerequisites:

- Not deleted already
- At least one recovery point is available

Cancel Recovery

Lets you stop recovery of the source.

Prerequisites: Cancel Recovery option is visible only when the source meets following prerequisites:

- Not deleted already
- Active recovery job is available to the source

Delete

Lets you delete the selected source from the list.

Prerequisites: Delete option is visible only when the source meets following prerequisites:

- Not deleted already
- A backup job is not active
- Recovered resource is not running
- An in-progress recovery job to recover data is not active

Remove

Lets you remove the selected source from Console.

Prerequisite: Remove option is visible only when the source is already deleted.

Provision

Lets you provision for the source.

Prerequisites: Provision option is visible only when the source meets following prerequisites:

- Available in a Disaster Recovery policy
- A recovered resource is available
- Recovered Resource is not running
- Not deleted already
- At least one recovery point is available

Assign Policy

Lets you assign a policy to the source. From the dialog of Assign Policy, select a policy that you want to assign and click **Confirm**.

Prerequisites: Assign Policy option is visible only when the source meets following prerequisites:

- Agent-based source is selected
- Not deleted already
- Source is not in a policy when an in-progress recovery job is recovering data

Remove Policy

Lets you remove policy from a source.

Prerequisites: Remove Policy option is visible only when the source meets following prerequisites:

- Agent-based source is selected
- Not deleted already
- Source has a Policy
- Source is not being restored

Source Groups

From Configure>Source Groups, you can perform individual action that varies according to your role.

Delete Group

Lets you delete the user.

Prerequisite: Delete option is visible only when the selected user is not the logged user.

Recovered Resources

From Protect > Recovered Resources, you can perform individual action that varies according to your role.

Provision

Lets you start a Recovered VM from recovery point.

Prerequisites: The recovered VM is deprovisioned or has provisioning failed status.

Start

Lets you power on the Recovered VM.

Prerequisites: The recovered VM is stopped.

Stop

Lets you power off the Recovered VM.

Prerequisites: The recovered VM is started and integration service is running on the VM.

Hard Stop

Lets you turn off the Recovered VM.

Prerequisites: The recovered VM is started.

Restart

Lets you start the Recovered VM again.

Prerequisites: The recovered VM is started before.

Deprovision

Lets you release the resources used by the recovered VM.

Prerequisites: The recovered VM is stopped.

Remote Console

Lets you connect to the recovered VM.

Prerequisites: The recovered VM is started before.

Destinations

From Protect > Destinations, you can perform individual action that varies according to your role.

Edit

Lets you modify the destination setting.

Delete

Lets you delete the destination from the list.

Prerequisites: Possible to delete only when not used in policy and no job is running on that destination.

View recovery points

Lets you view the list of available recovery points.

Jobs

From Analyze > Jobs, you can perform individual action that varies according to your role.

Cancel job

Lets you cancel a job.

Prerequisites: The job has *Running*. status

View Log

Lets you view logs for the job available for backup / recovery / deploy policy job.

How to Perform Global Actions for Cloud Direct

You can perform multiple global actions when using Cloud Direct. For example, Upgrade Agent, Start Backup, Cancel recovery, Delete, and remove. Depending on the roles, the actions may vary. This topic describes how to perform a global action for a function and helps you understand related prerequisites. For example, global actions for Sources, Source Groups, Recovered Resources, Destinations and Jobs.

Sources

From Protect>Sources, you can perform multiple global actions that vary according to your role.

Upgrade Agent

Click to upgrade cloud direct replication agent for all the selected sources.

Prerequisites: Upgrade Agent option is visible only when the sources meets following prerequisites:

- Only Cloud Direct sources are selected
- Not deleted already
- Upgrade is available

Start Backup

Click to start backup for all the selected sources.

Prerequisites: Start backup option is visible only when the sources meet following prerequisites:

- Only Cloud Direct sources are selected
- Not deleted already
- A policy is assigned
- Recovered resource is not running
- An in-progress recovery job to restore data is not active

Cancel Backup

Click to cancel backup for all the selected sources.

Prerequisites: Cancel backup option is visible only when the sources meet following prerequisites:

- Only Cloud Direct sources are selected
- Not deleted already

Cancel Recovery

Click to cancel recovery for all the selected sources.

Prerequisites: Cancel Recovery option is visible only when the sources meet following prerequisites:

- Only Cloud Direct sources are selected
- Not deleted already
- Active recovery job is available to the source

Delete

Click to remove the selected source from the displayed list. After being deleted, the sources are highlighted and cannot continue backup but can still support to recover data.

Prerequisites when Cloud Direct sources are selected: Delete option is visible only when the sources meet following prerequisites:

- Not deleted already
- A recovery job is not active
- A backup job is not active
- Recovered resource is not running

Prerequisites when Cloud Hybrid sources are selected: Delete option is visible only when the sources meet following prerequisites:

- Not deleted already
- A replication-in job is not active

Remove

Click to remove the selected sources from Console.

Prerequisite: Remove option is visible only when the selected sources meet following prerequisites:

- Only Cloud Direct sources are selected
- Source is already deleted

Provision

Click to provision for all the selected sources.

Prerequisites: Provision option is visible only when the sources meet following prerequisites:

- Only Cloud Direct sources are selected
- Available in a Disaster Recovery policy
- A recovered resource is available
- Recovered Resource is not running
- Not deleted already
- At least one recovery point is available

Assign Policy

Click to assign the same policy to all the selected sources. From the dialog of Assign Policy, select a policy that you want to assign and click **Confirm**.

Prerequisites: Assign Policy option is visible only when the sources meet following prerequisites:

- Only Cloud Direct sources are selected
- Agent-based source is selected
- Not deleted already

Remove Policy

Click to remove policy together from all the selected sources.

Prerequisites: Remove Policy option is visible only when the sources meet following prerequisites:

- Only Cloud Direct sources are selected
- Agent-based source is selected
- Already deleted
- A policy is assigned

Recovered Resources

From Protect > Recovered Resources, you can perform global action that varies according to your role.

Provision

Lets you start selected Recovered VMs from recovery point.

Prerequisites: The recovered VMs are deprovisioned or have provisioning failed status.

Start

Lets you power on the selected Recovered VMs.

Prerequisites: The recovered VMs are stopped.

Stop

Lets you power off the selected Recovered VMs.

Prerequisites: The recovered VMs are started and integration service is running on the VMs.

Hard Stop

Lets you turn off the selected Recovered VMs.

Prerequisites: The recovered VMs are started.

Restart

Lets you start the selected Recovered VMs again.

Prerequisites: The recovered VMs are started before.

Deprovision

Lets you release the resources used by the recovered VMs.

Prerequisites: The recovered VMs are stopped.

Remote Console

Lets you connect to the recovered VMs.

Prerequisites: The recovered VMs are started before.

Destinations

From Protect > Destinations, you can perform global action that varies according to your role.

Delete

Lets you delete the selected destinations from the list.

Prerequisites: Possible to delete only when not used in policy and no job is running on selected destinations.

Jobs

From Analyze > Jobs, you can perform global action that varies according to your role.

Cancel job

Lets you cancel selected jobs.

Prerequisites: The jobs have *Running*. status

Chapter 10: Frequently Asked Questions

This section contains the following topics:

How to Manage Alerts

Alert icon is available on the top panel of the Console. From the icon, you can view the number of available alerts. Clicking the icon displays three categories with numbers, message, and action options. To close the categories, click again on the Alert icon.

Alerts view according to role:

- **Direct Customer:** Views all alerts of own organization.
- **MSP Admin:** Views alerts of all the organizations.
- **MSP Account Admin:** Views alerts of the organizations that the admin manages.
- **End-User Admin:** Views all alerts related to Jobs and Policy.

Alerts are categorized into following three types:

- **Critical:** Refers to information that needs immediate action.
- **Warning:** Refers to information that needs action.
- **Information:** Refers to general messages. For example, task completion messages.

Possible Action on Displayed Alert Messages

You can take collective or individual action on messages available under a category.

- **Acknowledge All:** For collective action on the messages of a category, click Acknowledge All to remove all messages from that category.
- **View Logs:** For individual action, this option is available only for messages categorized as Information. From the drop-down option of a message, clicking View Logs lets you view complete detail about the message on the Logs screen.
- **Acknowledge:** For individual action, this option is available for messages of all the three categories. From the drop-down option of a message, clicking Acknowledge lets you remove the message from the Alerts list. Alerts are acknowledged automatically after 24 hours and you can view the alerts of the last 24 hours only.

Next Step: View Alert Category and Types

View Alert Category and Types

Alerts are divided broadly into six categories. Every category is further classified into multiple alert types. For every alert, based on the severity type specific action is performed.

Alert Category, Types, and Description

Category	Type	Severity	Description	Action (View Log)
Jobs	Backup Success	Information	{SOURCE_ NAME} backup completed suc-cessfully.	Yes
	Missed Backup	Critical	Source may be disconnected, powered off, or running as a recovered resource at the time of the scheduled backup.	No
	Backup Failed	Critical	When backup fails to com-plete	Yes
	Backup Warning	Warning	When {SOURCE_ NAME} backup is complete with warnings.	Yes
	Backup Errors	Critical	When {SOURCE_ NAME} backup is complete with errors.	Yes
	Recovery Success	Information	{SOURCE_ NAME} recov-ery completes successfully.	Yes
	Recovery Failed	Critical	When Recovery fails to com-plete.	Yes

	Recovery Error	Critical	When recovery of {SOURCE_ NAME} is complete with errors.	Yes
	Recovery Warning	Warning	When recovery of {SOURCE_ NAME} is complete with warnings.	Yes
Policy	Policy Assignment Successful	Information	When assigning policy to [SOURCE_ NAME] is successful.	Yes
	Policy Assignment Failed	Critical	When an attempt to apply policy to {SOURCE_ NAME} failed.	Yes
	Policy Assignment Warnings	Warning	When an attempt to apply policy to {SOURCE_ NAME} completed with warnings.	Yes
Trial	Cloud Direct Trial Started	Information	Default alert as soon as the organization is enrolled.	No
	Cloud Direct Trial	Warning	This alert displays the number of days left for the trial to expire.	No
	Cloud Direct Trial Expiration	Critical	When the trial expired	No
	Cloud Hybrid Trial Started	Information	When the trial for Cloud Hybrid is activated	No
	Cloud Hybrid Trial	Warning	Displays the number of days	No

			left for Cloud Hybrid trial to expire	
	Cloud Hybrid Trial Expiration	Critical	When the Cloud Hybrid trial expired	No
Storage – Cloud Direct	Approaching Storage Capacity	Warning	Cloud Direct usage at {x%} capacity	No
	Storage Capacity Exceeded	Critical	Cloud Direct storage capacity reached	No
Storage – Cloud Hybrid	Approaching Storage Capacity	Warning	Cloud Hybrid usage at {x%} capacity	No
	Storage Capacity Exceeded	Critical	Cloud Hybrid storage capacity reached	No
Configuration	Cloud Direct DR Configuration	Information	Your organization has DRaaS capability. Please contact the Support team to set up your Virtual Private Cloud.	No
		Warning	When DR is activated and DR configuration is incomplete, a message is displayed: Your disaster recovery environment has not been fully configured. Please contact the Arcserve Support team to set up your Virtual Private Cloud.	No

	Cloud Hybrid Configuration	Warning	When CH is activated and CH configuration is incomplete, a message is displayed: Your Cloud Hybrid environment has not been fully configured. Please contact the Arcserve Support team to set up your Cloud Hybrid data store.	No
Licensing	Cloud Direct License	Warning	This alert displays the number of days (that is, last 30 days) left for the Cloud Direct license to expire.	No
	Cloud Hybrid License	Warning	This alert displays the number of days (that is, last 30 days) left for the Cloud Hybrid license to expire.	No
Suspend	Organization	Critical	Your account has been suspended and your backups have been disabled. Please contact your provider for details.	No

How to Create a New Account

You can create a new account from the login page of Arcserve® Business Continuity Cloud. The new account can belong to any role of Arcserve® Cloud.

Note: A default policy and destination are created by default when a new organization or account is created.

Follow these steps:

1. Open Arcserve® Business Continuity Cloud login screen.
2. From the login screen, click **Don't have an account? Sign up now!**
3. From the Enroll pane of Personal Information, perform the following steps:
    a. Enter personal details.
    b. Select check box of MSP/Reseller if applicable.
    c. Select check box to agree to Terms of Service.
    d. Click **Next**.

    Select Region pane appears.
4. Select the location to store the backup data and click **Next**.

    The confirmation message appears.
5. From the Email ID provided during enrollment, open the email from Arcserve® Business Continuity Cloud.
6. Click the Activation link and follow the instructions to complete registration.

You can change or reset your password later.

How to Change or Reset Password

After creating your account, you can either change your password from the Console or reset password from the login screen.

Change Password

Follow these steps:

1. Log into the Console, navigate to the User Login icon from top-right corner and click **User Profile**.
2. From **My Profile** screen, under Change Password, provide **Current Password** , enter **New Password** twice and click **Update Password**.

   The password is updated.

Reset Password

You can reset your password from Arcserve Cloud Console login screen.

Follow these steps:

1. Open Arcserve® Business Continuity Cloud login screen.
2. From the login screen, click **Forgot password? Click here!**
3. From the **Reset Password** dialog, enter your registered Email and click **Reset**.

   An email is sent to your registered email ID.
4. From your inbox, follow the instructions in reset password email to set a new password and log into Arcserve Cloud Console.

   Note: Before you reset the password using the link in email, you can still use the old password if you remember.

How to Save a Search

Saving a search often helps later when you are handling huge set of data. Arcserve® Business Continuity Cloud not only helps you save a search with all results but also lets you manage saved searches.

Arcserve® Business Continuity Cloud reduces your multiple search efforts. From the Console, you can opt to save search results with a unique name. When you *perform a search*, the search results appear on the screen and the search term is displayed below the Search box at the **Search results for:** option. You can opt to either **Clear All** search terms or **Save Search**.

To save, click **Save Search**. A dialog for Save Search appears. Enter a unique name in the **Save Search Name** box and click **Save Search**. A message confirms successful action. The saved search name appears always in front of **Saved Searches**. You can click the name to view results even later without having to repeat the search.

How to use Retention Settings

Retention settings allow to specify the duration of time to keep data associated with recovery points stored within a volume. When the specified length of time elapses, the recovery point is deleted with the related associated data.

Retention settings include the current time period. For example, **Keep monthlies for 2 months** retains monthly recovery point for the current month and also the monthly recovery point for the previous month.

Note: Keeping more recovery points for longer periods of time may result in increased consumption of cloud storage depending on the data change rate between recovery points.

How to Add Throttling Schedule

Throttle schedule lets you control the data transfer to cloud throughput speed that in turn controls the resource usage (network bandwidth) of the server being transfer to cloud. This schedule is useful if you do not want to affect the server performance during business hours. You can add four time windows per day in your data transfer to cloud throttling schedule. For each time window, you can specify a value, in kbits per second. This value is used to control the transfer to cloud throughput. Valid values start from 300 kbits.

If the data transfer job extends its specified time, then the throttle limit adjusts according to the specified time window. For example, you have defined the data transfer throttle limit as 500 kbits from 8:00 AM to 8:00 PM, and 2500 kbits from 8:00 PM to 10:00 PM. If a data transfer job starts at 7:00 PM and runs for three hours, then from 7:00 PM to 8:00 PM the throttle limit is 500 kbits and from 8:00 PM to 10:00 PM the throttle limit is 2500 kbits.

If more than one source node exists in the backup task with virtual standby to the cloud, the nodes divide throttle limit equally. For example, you have defined the data transfer throttle limit as 500 kbits and two source nodes exist in the plan. When the nodes transfer data to cloud simultaneously, the throttle limit is 250 kbits for every node. When tansfer from one node is complete, the other running node's throttle limit changes to 500 kbits.

If you do not define any throttling schedule, the data transfer to cloud job runs at maximum speed.

Follow these steps:

1. From the Schedule option screen, click **Add** for Throttle Schedule.
2. Perform the following steps:
   - Enter **Throughput Limit**. Minimum value is 300.
   - Select All or name of specific days for **Run Schedule**.
   - Enter **Start Time** and **End Time**.

How to Suspend Organization

MSP Admin or MSP Account Admin is allowed to suspend the customer account. To suspend, from the **Action** drop-down list, click **Suspend**.

This section contains the following topics:

Suspend Organization

MSP Admin or MSP Account Admin is allowed to suspend the customer account.

After the customer account is suspended, the following effects takes place:

In Customer Organizations,

- All the policies present in the organization gets disabled.
- Policies cannot be created, edited, and deleted.
- The following backup jobs does not work:
  - On Demand backup
  - Scheduled jobs

  If the backup job is in progress state, the job status shows as cancel and alerts will be generated to the customer account in Failure state.
- Recovery jobs gets restored.
- An Alert is triggered to the customer account stating that your account is suspended.

- The Customer Admin, MSP admin (View as End-User Admin), or MSP Account Admin (View as End-User Admin) can create, edit, and delete the following:
  - Destinations
  - Sources
  - Groups
  - Filters
  - Users
  - Reports
  - Alerts

How to Enable Organization

MSP Admin or MSP Account Admin is allowed to resume the suspended customer account. To Resume, from the **Action** drop-down list, click **Enable**.

This section contains the following topics:

Enable Organization

MSP Admin or MSP Account Admin is allowed to resume the suspended customer Accounts.

After the customer account is enabled, the following effects takes place:

In Customer Organizations,

- All the operations continues normally.
- All the policies present in the organization gets enabled.
- Backup Jobs run normally.
- Recovery jobs run normally.

- The Customer Admin, MSP admin (View as End-User Admin), or MSP Account Admin (View as End-User Admin) can create, edit, and delete the following:
  - Policies
  - Destinations
  - Sources
  - Groups
  - Filters
  - Users
  - Reports
  - Alerts

How to enable or disable a policy

This section provides information about enabling or disabling a policy using the **Policies** screen.

This section contains the following topics:

Enable Policy

To enable a policy, from the **Policies** screen, using the **Action** drop-down list, click **Enable**.

Before you enable a policy, consider the following:

- MSP Admins enable policies of Customer Accounts that are disabled by Customer Admin/MSP Admin/MSP Account Admin.
- MSP Account Admins enable policies of assigned Customer Account.
- MSP Account Admins enable policies that are disabled by Customer Admin/MSP Admin/MSP Account Admin.
- Customer Admin enable policies that are disabled by the same user or other Customer Admins of their respective organization.
- Direct Admin enable policies that are disabled by the same user or other Direct Admins of their respective organization.

Disable Policy

To disable a policy, from the **Policies** screen, using the **Action** drop-down list, click **Disable**.

Before you disable a policy, consider the following:

- Customer Admin disable policies in their respective organization.
- Direct Admin disable policies in their respective organization.
- MSP Admins disable policies of all Customer Accounts.
- MSP Account Admins disable policies of assigned Customer Account.